UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO TECNOLÓGICO
DEPARTAMENTO DE ENGENHARIA DO CONHECIMENTO
CURSO DE ESPECIALIZAÇÃO EM INTELIGÊNCIA E INOVAÇÃO APLICADAS NO ENFRENTAMENTO AO CRIME ORGANIZADO

Elias Milhomens de Araújo
Felipe Cesar Gonçalves de Mendonça

Ação do Crime Organizado em Infraestruturas Críticas: Ataques a Serviços Essenciais e seus Impactos na Segurança Pública

Florianópolis/SC
2026

Elias Milhomens de Araújo
Felipe Cesar Gonçalves de Mendonça

Ação do Crime Organizado em Infraestruturas Críticas: Ataques a Serviços Essenciais e seus Impactos na Segurança Pública

Trabalho de Conclusão de Curso submetido ao curso de Especialização em Inteligência e Inovação Aplicadas no Enfrentamento ao Crime Organizado, do Centro Tecnológico da Universidade Federal de Santa Catarina como requisito parcial para a obtenção do título de especialista em Inteligência e Inovação Aplicadas no Enfrentamento ao Crime Organizado.

Orientador: Prof. Alexandre Leopoldo Gonçalves, Dr.

Florianópolis/SC
2026

Araújo, Elias Milhomens de
Ação do Crime Organizado em Infraestruturas Críticas : Ataques a Serviços Essenciais e seus Impactos na Segurança Pública / Elias Milhomens de Araújo, Felipe Cesar Gonçalves de Mendonça ; orientador, Alexandre Leopoldo Gonçalves, 2026.
40 p.

Monografia (especialização) - Universidade Federal de Santa Catarina, Centro Tecnológico, Curso de Inteligência e Inovação Aplicadas no Enfrentamento ao Crime Organizado, Florianópolis, 2026.

Inclui referências.

1. Segurança Pública. 2. Crime Organizado. 3. Ataque. 4. Infraestruturas Críticas. 5. Serviços Essenciais. I. Mendonça, Felipe Cesar Gonçalves de. II. Gonçalves, Alexandre Leopoldo. III. Universidade Federal de Santa Catarina. Inteligência e Inovação Aplicadas no Enfrentamento ao Crime Organizado. IV. Título.

Elias Milhomens de Araújo
Felipe Cesar Gonçalves de Mendonça

Ação do Crime Organizado em Infraestruturas Críticas: Ataques a Serviços Essenciais e seus Impactos na Segurança Pública

Este Trabalho de Conclusão de Curso foi julgado adequado para obtenção do título de especialista em Inteligência e Inovação Aplicadas no Enfrentamento ao Crime Organizado e aprovado em sua forma final pelo Curso de Especialização em Inteligência e Inovação Aplicadas no Enfrentamento ao Crime Organizado.

Florianópolis, 09 de março de 2026.

Documento assinado digitalmente
Marcelo Macedo
Data: 24/03/2026 12:38:27-0300
CPF: ***.190.199-**
Verifique as assinaturas em https://v.ufsc.br

Coordenação do Curso

Banca examinadora

Documento assinado digitalmente
Alexandre Leopoldo Goncalves
Data: 24/03/2026 12:24:24-0300
CPF: ***.740.349-**
Verifique as assinaturas em https://v.ufsc.br

Prof. Alexandre Leopoldo Gonçalves, Dr.
Universidade Federal de Santa Catarina
Orientador

Documento assinado digitalmente
THIAGO DOMINGOS MARQUES
Data: 24/03/2026 11:01:53-0300
CPF: ***.711.039-**
Verifique as assinaturas em https://v.ufsc.br

Thiago Domingos Marques, Me.
Avaliador

AÇÃO DO CRIME ORGANIZADO EM INFRAESTRUTURAS CRÍTICAS: ATAQUES A SERVIÇOS ESSENCIAIS E SEUS IMPACTOS NA SEGURANÇA PÚBLICA.

ORGANIZED CRIME ACTION IN CRITICAL INFRASTRUCTURES: ATTACKS ON ESSENTIAL SERVICES AND THEIR IMPACT ON PUBLIC SAFETY.

Elias Milhomens de Araújo[1]
Felipe Cesar Gonçalves de Mendonça[2]

RESUMO

Atualmente, a proteção das infraestruturas críticas cresce como uma das principais preocupações dos Estados modernos. A digitalização de processos e a internet das coisas agiliza e facilita o gerenciamento de serviços essenciais e, ao mesmo passo, representam uma grande vulnerabilidade em face de ações coordenadas da criminalidade organizada com o objetivo de desestabilizar a ordem social dos países. Nesse sentido, o objetivo deste estudo é mapear o cenário atual do Brasil na proteção das infraestruturas críticas, especialmente em face de ações da criminalidade organizada. Para tal, utilizou-se uma revisão integrativa da literatura recente nacional e internacional visando identificar como o tema é tratado em diversos países, bem como as diferentes abordagens adotadas pela academia a depender do escopo científico adotado. Os autores ligados a órgãos e entidades de proteção estatal adotam uma posição de análise casuístico-documental retrospectiva, indicando os estados como principais agentes no processo; ao passo que os autores dos ramos da engenharia e ciência da computação adotam uma visão ampla e prospectiva, propondo abordagens preditivas das vulnerabilidades por meio da utilização de novas tecnologias e com maior ênfase nos atores privados. De todo o apurado foi possível concluir que o Brasil passou a olhar e buscar a sistematização da proteção das infraestruturas críticas a partir de ataques de organizações criminosas ao sistema público de transporte. Desde então, ao longo dos anos, o país avançou na regulação da atividade, contudo, ainda carece de amadurecimento do papel estatal na coordenação e centralização dos esforços, especialmente após os programas de descentralização da prestação dos serviços essenciais à iniciativa privada.

Palavras-chave: crime organizado; ataque; ameaça; infraestruturas críticas; serviços essenciais.

ABSTRACT

At present, the protection of critical infrastructures has emerged as one of the foremost concerns of modern states. The digitalization of processes and the expansion of the Internet of Things streamline and facilitate the management of essential services; at the same time, however, they introduce significant vulnerabilities to coordinated actions by organized criminal groups seeking to undermine social order. Against this backdrop, this study aims to map the current situation in Brazil regarding the protection of critical infrastructures, with particular attention to threats posed by organized crime. To this end, an integrative review of recent national and international literature was conducted in order to examine how the issue is

[1] Delegado de Polícia Federal – Polícia Federal. Especialista em Gestão Integrada de Inteligência. Agência Brasileira de Inteligência. Especialista em Investigação Criminal. Universidade Católica de Brasília – Polícia Civil do Distrito Federal.

[2] Delegado de Polícia Civil do Maranhão - Coordenador do Centro Integrado de Inteligência do Nordeste/DIOPI/MJSP

addressed in different countries, as well as the distinct approaches adopted within the academic literature depending on the scientific scope pursued. Authors affiliated with state protection agencies and institutions tend to adopt a retrospective, case-based and documentary analytical perspective, identifying the state as the central actor in this process. By contrast, scholars in the fields of engineering and computer science take a broader and more forward-looking view, proposing predictive approaches to vulnerability assessment through the use of emerging technologies and placing greater emphasis on the role of private-sector actors. Overall, the findings indicate that Brazil began to turn its attention to, and to pursue the systematization of, critical infrastructure protection in response to attacks by criminal organizations on the public transportation system. Since then, the country has made progress in regulating this area; nevertheless, it still lacks a more mature articulation of the state's role in coordinating and centralizing efforts, particularly in the wake of policies that have decentralized the provision of essential services to the private sector.
Keywords: organized crime; attack; threat; critical infrastructure; essential services.

1 INTRODUÇÃO

A segurança das infraestruturas críticas consolidou-se como uma preocupação central dos Estados contemporâneos diante da crescente complexidade e interdependência dos sistemas responsáveis pela prestação de serviços essenciais à sociedade (OECD, 2019; United States, 2023). Setores como telecomunicações, energia, transportes, saúde, abastecimento e serviços digitais passaram a operar como sistemas sociotécnicos altamente integrados, cuja interrupção ou degradação pode produzir efeitos sistêmicos sobre a ordem social, a estabilidade econômica e a governabilidade (Rinaldi; Peereboom; Kelly, 2001; European Commission, 2020).

A digitalização intensiva desses serviços, impulsionada pela automação industrial, pela Internet das Coisas (do inglês *Internet of Things* - IoT) e pela convergência entre ambientes físicos e cibernéticos, ampliou significativamente a superfície de ataque e redefiniu o próprio conceito de vulnerabilidade estrutural (Wendt, 2011; Enisa, 2022). Nesse contexto, infraestruturas críticas deixaram de ser apenas ativos estratégicos do Estado para se tornarem pontos sensíveis de disputa, exploração e coerção por parte de atores estatais e não estatais (Guterres, 2016; Gülcan *et al.*, 2023).

Como decorrência de tal cenário há o paradoxo da digitalização, uma vez que a IoT, ao passo que traz agilidade e automatização de processos, implica na criação e incremento vulnerabilidades decorrentes da inserção de estruturas em ambiente cibernético, altamente suscetível a ataques e investidas da criminalidade organizada.

Há, nesse cenário, uma crescente preocupação de que tais vulnerabilidades sejam utilizadas cada vez mais pelo crime organizado como forma de ataque a infraestruturas essenciais, promovendo a desestabilização do Estado constituído e a promoção de pânico generalizado.

A literatura internacional identifica como principais desafios a fragmentação institucional dos modelos de proteção, a dificuldade de coordenação interagências, a assimetria de capacidades entre o poder público e operadores privados e a emergência de ameaças híbridas, que combinam ataques físicos, cibernéticos e informacionais (OECD, 2019; Udeanu, 2015). Organismos como a Organização para a Cooperação e Desenvolvimento Econômico (do inglês *Organisation for Economic Co-operation and Development* - OECD) e a União Europeia (do inglês *European Union* - EU) apontam que a governança das

infraestruturas críticas enfrenta limitações estruturais relacionadas à soberania nacional, à proteção de dados sensíveis e ao compartilhamento de informações estratégicas (EU, 2016; OECD, 2020).

Em resposta, países como Estados Unidos, Alemanha e Reino Unido avançaram na criação de agências nacionais especializadas e de marcos regulatórios voltados à gestão integrada de riscos, à inteligência de ameaças e à cooperação público-privada (United States, 2018; BMI, 2021), enquanto a EU tem buscado harmonizar padrões mínimos de segurança por meio de diretivas como a NIS (Network and Information Security) e a NIS2 (EU, 2016; EU, 2022).

Paralelamente, observa-se o crescimento de estratégias baseadas em soluções tecnológicas avançadas, como Inteligência Artificial (do inglês *Artificial Intelligence* - AI), Aprendizado de Máquina (do inglês *Machine Learning* - ML) e arquiteturas distribuídas, orientadas à detecção precoce de anomalias e ao aumento da resiliência sistêmica (Lozano; Llopis; Domingo, 2023; Govea; Gaibor-Naranjo; Villegas-Ch, 2024).

No Brasil, a agenda de proteção das infraestruturas críticas ganhou relevância sobretudo a partir de episódios concretos de ataques promovidos por organizações criminosas, como os eventos ocorridos no estado de São Paulo em 2006, que evidenciaram a capacidade desses grupos de impactar serviços essenciais como forma de pressão e desestabilização social (Siqueira; Nascimento; Moraes, 2022; Miranda Filho, 2012). Desde então, o país estruturou um conjunto de instrumentos normativos, incluindo a Política Nacional de Segurança de Infraestruturas Críticas (PNSIC) (Brasil, 2018), a Estratégia Nacional (Brasil, 2020) e o Plano Nacional (Brasil, 2022a), que estabeleceram princípios, objetivos e diretrizes para a proteção desses ativos.

Apesar desses avanços, estudos institucionais e acadêmicos indicam que o modelo brasileiro permanece marcado por dispersão de competências, ausência de uma autoridade central permanente e forte dependência de arranjos episódicos. Isso ocorre, especialmente, em um cenário em que grande parte das infraestruturas essenciais é operada por agentes privados, nacionais e estrangeiros, com integração limitada aos sistemas estatais de inteligência e segurança (Nonato; Pinho, 2021; Inacio; Silva, 2023).

Diante desse cenário, o objetivo deste trabalho é analisar a atuação de organizações criminosas em face das infraestruturas críticas no Brasil, com ênfase para os ataques aos serviços essenciais. Assim como, identificar padrões de atuação, vulnerabilidades estruturais, mecanismos de proteção existentes e o nível de maturidade institucional do Estado brasileiro para prevenir, mitigar e responder a esse tipo de ameaça. Busca-se, ainda, situar o caso brasileiro em perspectiva quanto às estratégias adotadas no plano internacional, de modo a contribuir para o aprimoramento das políticas públicas de segurança e resiliência de infraestruturas críticas.

Para atingir esse objetivo, o artigo está organizado da seguinte forma: a Seção 2 apresenta a fundamentação teórica, abordando os principais conceitos e debates sobre infraestruturas críticas, segurança e criminalidade organizada. A Seção 3 descreve os procedimentos metodológicos adotados, com destaque para a revisão integrativa realizada. A Seção 4 desenvolve a análise e discussão dos resultados, estruturada em dimensões que contemplam o marco normativo, o foco geopolítico, os atores criminosos, os modos de ataque e os principais achados da literatura. Por fim, a Seção 5 apresenta as conclusões e discute as implicações dos resultados para a formulação e o fortalecimento de políticas públicas voltadas à proteção das infraestruturas críticas no Brasil.

2 FUNDAMENTAÇÃO TEÓRICA

Nesta seção, serão apresentados os principais conceitos relacionados às infraestruturas críticas, à sua classificação no ordenamento jurídico brasileiro e às noções de ameaça, vulnerabilidade e interdependência sistêmica, a fim de estabelecer as bases analíticas necessárias à compreensão das estratégias adotadas por atores criminosos nesse contexto. Busca-se, portanto, delimitar o campo teórico e institucional que orienta a análise subsequente, conferindo densidade conceitual ao debate e assegurando coerência com o desenvolvimento argumentativo do artigo.

2.1 CONCEITO DE ORGANIZAÇÃO CRIMINOSA ADOTADO NO BRASIL

A partir de compromissos internacionais de enfrentamento à criminalidade organizada, os estados aderentes adotaram em seus sistemas jurídicos internos regras acerca do conceito e dos efeitos legais e de persecução penal das organizações criminosas.

Segundo Zilio (2025), o sistema jurídico penal brasileiro, quanto à criminalidade organizada, define essencialmente a previsão de três modalidades de organização criminosa em sentido amplo: constituição de milícias (art. 288-A do CPB), organização criminosa em sentido estrito (artigo 2º da Lei 12.850/2013 (Brasil, 2013)) e organização terrorista (art. 3º da Lei 13.260/2016).

A Lei 12.850/2013, que é o diploma nacional dedicado essencialmente ao enfrentamento às organizações criminosas, conceituando-as como uma associação de quatro ou mais pessoas estruturalmente ordenada e caracterizada pela divisão de tarefas, ainda que informalmente, com objetivo de obter, direta ou indiretamente, vantagem de qualquer natureza, mediante a prática de infrações penais cujas penas máximas sejam superiores a quatro anos, ou que sejam de caráter transnacional.

O crime de associação criminosa, voltado a grupos menos estruturados dedicados à prática de crimes, constitui-se da associação de três ou mais pessoas para a prática de crimes, não tendo como elemento a divisão de tarefas, a obtenção de vantagem de qualquer natureza e que os crimes cometidos ou pretendidos sejam transnacionais ou com pena superior a quatro anos. A milícia constitui-se de organização criminosa de caráter paramilitar, de milícia particular, de grupo ou de esquadrão com a finalidade de praticar qualquer dos crimes previstos no Código Penal. Já a organização criminosa terrorista é assim considerada caso seja voltada a prática, por um ou mais indivíduos, dos atos previstos na lei, por razões de xenofobia, discriminação ou preconceito de raça, cor, etnia e religião, quando cometidos com a finalidade de provocar terror social ou generalizado, expondo a perigo pessoa, patrimônio, a paz pública ou a incolumidade pública.

Camargo *et al*. (2020) defendem que essas definições correspondem aos parâmetros estabelecidos internacionalmente pela Convenção das Nações Unidas contra o Crime Organizado Transnacional. Cabe mencionar que sua adoção pelo legislador brasileiro foi endossada por anos de discussão entre doutrina e jurisprudência em torno da necessidade ou não de uma tipificação mais complexa do fenômeno do que aquela oferecida pela redação do antigo crime de quadrilha ou bando, do Código Penal.

No trabalho de Annibal (2022), o autor tece relevante crítica ao modelo adotado pelo Brasil, pontuando que, assim como a própria criminologia ainda encontra obstáculos na delimitação conceitual precisa do que se entende por organização criminosa, os governos demonstram limitações ainda mais acentuadas na compreensão estrutural e funcional desses agrupamentos ao formular políticas públicas de enfrentamento. A insuficiência de diagnóstico

qualificado tende a conduzir à adoção de respostas simplificadas e de forte apelo político, que privilegiam estratégias repressivas de curto prazo. O resultado, frequentemente, é o incremento do encarceramento em massa de segmentos socialmente vulneráveis, sem a desarticulação efetiva das cadeias de comando e financiamento, o que, paradoxalmente, contribui para o fortalecimento e a expansão das próprias facções criminosas.

No mesmo sentido, Salla *et al*. (2020) destacam a existência de uma corrente discursiva, amplificada pelos meios de comunicação, que concentra sobre as periferias urbanas, sobre a população carcerária e sobre os operadores do varejo do tráfico de drogas a imputação genérica de "crime organizado". De modo geral, associando-lhes a responsabilidade pelas múltiplas manifestações da violência urbana. Tal dinâmica decorre de um processo de eufemização e ocultamento da criminalidade econômica estruturada, acompanhado da superexposição dramatizada da criminalidade comum, que passa a ocupar o lugar de arquétipo da delinquência no imaginário social e nas agendas institucionais de controle.

Essa distorção interpretativa possui reflexos diretos quando se desloca a análise para o campo das Infraestruturas Críticas (ICs). Conforme observa Sá (2017), o Brasil ainda apresenta déficit de produção acadêmica e de formulação civil estruturada sobre o tema, permanecendo o debate concentrado, em grande medida, nos segmentos militares e em círculos técnicos restritos. A prevalência de uma leitura simplificada do fenômeno criminal — centrada no varejo do tráfico e na criminalidade ostensiva — contribui para obscurecer ameaças mais complexas, como aquelas que incidem sobre ativos estratégicos e serviços essenciais, dificultando a construção de políticas públicas orientadas à proteção sistêmica e à resiliência nacional.

Citando a Política Nacional de Segurança das Infraestruturas Críticas, Okabayashi (2024) aponta que, no Brasil, é fomentada a articulação coordenada entre órgãos estatais, iniciativa privada e sociedade civil com o objetivo de mapear vulnerabilidades e implementar medidas de mitigação baseadas em metodologias estruturadas de análise e gestão de riscos. Ainda, acrescenta Sá (2017), que são consideradas críticas as infraestruturas cuja importância estratégica é fundamental não apenas para garantir a segurança e soberania do País, mas também para promover a integração e o desenvolvimento econômico sustentável, conceito este previsto no art. 1º do Decreto nº 9.573, de 22 de Novembro de 2018 (Brasil, 2018).

2.2 MARCO NORMATIVO DA PROTEÇÃO DE INFRAESTRUTURAS CRÍTICAS NO BRASIL

O arcabouço normativo de proteção das ICs representa o ecossistema essencial para a implementação da resiliência. O Brasil possui uma série de normativos específicos, que apresentam as diretrizes de proteção das ICs, destacando a importância da colaboração entre o setor de defesa, a comunidade acadêmica e os setores público e privado (Neves, 2024).

O Decreto nº 9.573, de 22 de novembro de 2018 aprovou a PNSIC, instituída pelo Gabinete de Segurança Institucional da Presidência da República por meio do Decreto nº 9.573, de 22 de novembro de 2018 (Brasil, 2018). O Decreto e seu anexo representam a base nacional para as ações voltadas à segurança das infraestruturas críticas. Nas Disposições Gerais, a PNSIC apresenta os conceitos necessários à sua implementação:

> I - **infraestruturas críticas** - instalações, serviços, bens e sistemas cuja interrupção ou destruição, total ou parcial, provoque sério impacto social, ambiental, econômico, político, internacional ou à segurança do Estado e da sociedade;

> II - **segurança de infraestruturas críticas** - conjunto de medidas, de caráter preventivo e reativo, destinadas a preservar ou restabelecer a prestação dos serviços relacionados às infraestruturas críticas;
> III - **interdependência de infraestruturas críticas** - relação de dependência ou interferência de uma infraestrutura crítica em outra ou de uma área prioritária de infraestruturas críticas em outra; e
> IV - **resiliência** - capacidade de as infraestruturas críticas serem recuperadas após a ocorrência de situação adversa. [grifo nosso].

Nota-se que dos quatro conceitos apresentados, três deles dizem respeito a protocolos de segurança e proteção das infraestruturas. No mesmo sentido, a política nacional estabelece como princípios a "prevenção e a precaução, com base na análise de riscos", a "integração entre as diferentes esferas do Poder Público, o setor empresarial e os demais segmentos da sociedade" e a "salvaguarda do interesse da defesa e da segurança nacional".

Na definição de seus objetivos, a PNSIC dedica especial atenção à prevenção, proteção e manutenção das atividades relacionadas às infraestruturas críticas:

> I - a **prevenção de eventual interrupção, total ou parcial**, das atividades relacionados às infraestruturas críticas ou, no caso de sua ocorrência, a **redução dos impactos** dela resultantes;
> II - o estabelecimento de diretrizes e instrumentos para **salvaguardar as infraestruturas críticas consideradas indispensáveis** à segurança nacional;
> III - a integração de dados sobre ameaças, tecnologias de segurança e **gestão de riscos**;
> IV - a identificação das relações de interdependência entre as infraestruturas críticas no País;
> V - o desenvolvimento, com enfoque na **prevenção**, de uma consciência acerca da **segurança de infraestruturas críticas**; e
> VI - o estabelecimento da **prevalência do interesse da defesa e da segurança nacional na proteção, na conservação e na expansão** das infraestruturas críticas. [grifo nosso].

Para tanto, a PNSIC aponta como seus instrumentos: i) a Estratégia Nacional de Segurança de Infraestruturas Críticas; ii) o Plano Nacional de Segurança de Infraestruturas Críticas; e iii) o Sistema Integrado de Dados de Segurança de Infraestruturas Críticas".

A Estratégia Nacional de Segurança de Infraestruturas Críticas (Brasil, 2020a) possui natureza conceitual e principiológica, trazendo conceitos, princípios e objetivos da segurança de infraestruturas críticas numa abordagem ampla. Já o Plano Nacional de Segurança de Infraestruturas Críticas foi aprovado pelo Decreto nº 11.200, de 15 de setembro de 2022 (Brasil, 2022a), e também prevê o Sistema Integrado de Dados de Segurança de Infraestruturas Críticas. O documento possui natureza conceitual operacional, delineando em viés operacional, atribuições e responsabilidades, planos setoriais, estaduais e municipais, ações estratégicas e diretrizes de gerenciamento da segurança das infraestruturas críticas do país.

Em 2024, o Governo Federal, por meio de Portaria Interministerial (Brasil, 2024) instituiu o Comitê Nacional de Segurança de Infraestruturas Críticas no âmbito da Câmara de Relações Exteriores e Defesa Nacional do Conselho de Governo. O Comitê foi instituído com o objetivo de monitorar a implementação e a evolução da PNSIC. Ele é presidido pelo GSI,

composto por representantes da Casa Civil da Presidência da República; do Ministério da Agricultura e Pecuária; do Ministério das Cidades; do Ministério da Ciência, Tecnologia e Inovação; do Ministério das Comunicações; do Ministério da Defesa; do Ministério da Fazenda; do Ministério da Gestão e da Inovação em Serviços Públicos; do Ministério da Integração e do Desenvolvimento Regional; do Ministério da Justiça e Segurança Pública; do Ministério de Minas e Energia; do Ministério de Portos e Aeroportos; do Ministério da Saúde; do Ministério dos Transportes; da Agência Brasileira de Inteligência; do Comando da Marinha; do Comando do Exército; e do Comando da Aeronáutica.

Analisando-se todo o arcabouço normativo, conceitual, principiológico e estratégico mencionado, nota-se que há uma natureza difusa, sem existência de órgão capaz de centralizar o controle da segurança das infraestruturas críticas do país, uma vez que o GSI é apontado apenas como órgão "articulador" da atividade de segurança de infraestruturas críticas. Tal fato ocorre devido a gama de serviços que se inserem nesse conceito, abrangendo atividades que podem estar sendo prestadas diretamente por entes ou entidades estatais ou mesmo terem sido objeto de concessão ou privatização a particulares.

Não por outro motivo, a ENSIC (Brasil, 2020a) traz como princípio a "atuação integrada", pontuando que a maior parte das infraestruturas críticas nacionais se encontram sob propriedade ou operação do setor privado, exigindo a adoção de um modelo cooperativo, pressupondo mecanismos permanentes de compartilhamento de informações estratégicas entre os atores envolvidos.

Por fim, o GSI da Presidência da República figura como órgão articulador da atividade de segurança de infraestruturas críticas, responsável pela implementação do Sistema Integrado de Dados de Infraestruturas Críticas instituído no âmbito da PNSIC, com a finalidade de consolidar e sistematizar informações estratégicas relativas aos setores considerados essenciais à segurança nacional, conforme previsto no Decreto nº 9.573, de 22 de novembro de 2018, do GSI da Presidência da República (Brasil, 2018).

2.3 INFRAESTRUTURAS CRÍTICAS (IC) E INTERDEPENDÊNCIAS

A proteção das Infraestruturas Críticas (do inglês *Critical Infrastructure* - CI) fundamenta-se na identificação, classificação e proteção de ativos, sistemas e redes cuja interrupção, degradação ou destruição possa comprometer de maneira significativa a continuidade de funções essenciais do Estado e da sociedade. Especialmente, encontra-se nesse rol aquelas CIs relacionadas à segurança nacional, à ordem pública e à estabilidade econômica, conforme estabelecido na PNSIC (Brasil, 2018) e reiterado no plano internacional pela diretiva (EU) 2022/2557 sobre a resiliência de entidades críticas (EU, 2022).

Diferentemente da concepção tradicional, centrada na proteção de instalações físicas isoladas, a abordagem contemporânea desloca o foco para a salvaguarda de serviços essenciais e dos fluxos que os sustentam — como energia, dados, mobilidade, água e capital —. Compreende ainda, as infraestruturas como sistemas sociotécnicos complexos, interdependentes e fortemente ancorados em tecnologias digitais, conforme delineado no *National Infrastructure Protection Plan* do *Department of Homeland Security* (United States, 2013) e na Diretiva (UE) 2022/2557 do European Union (EU, 2022 A ênfase desloca-se da proteção patrimonial para a resiliência sistêmica, entendida como a capacidade de prevenir, absorver e recuperar-se de disrupções.

Sá (2017) apresenta um quadro comparativo entre alguns países do mundo, destacando os serviços que se constituem como infraestrutura crítica (Quadro 1). Entre os

exemplos, na maioria dos países estão o sistema bancário, as telecomunicações, o transporte, a distribuição de água, a distribuição de energia, a agricultura e o sistema de saúde.

Quadro 1 - Setores considerados críticos em diversos países

PAÍSES / **SECTORES**	AUS	AUT	BRA	CAN	EST	FRA	FIN	DEU	HUN	IND	ITA	JPN	KOR	MAL	NLD	NOR	NZL	POL	RUS	SWE	SGP	ESP	CHE	GBR	USA
Banca e Finanças	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Governo Central		X		X	X	X		X	X		X	X	X	X	X	X	X	X	X	X		X	X	X	X
Indústria Química e Nuclear				X						X				X	X			X				X	X		X
Serviços de Emergência	X		X	X	X	X			X	X	X		X	X		X	X	X	X			X	X	X	X
Electricidade/Energia	X	X		X	X	X	X	X	X	X	X	X	X		X	X	X	X			X	X	X	X	X
Agricultura/Alimentação	X			X	X	X	X	X	X		X	X			X	X					X	X	X	X	X
Serviços de Saúde	X		X	X	X	X	X		X		X			X	X	X					X	X	X	X	X
Comunicação/Media	X	X				X	X		X		X		X		X	X			X	X	X		X		X
Defesa						X			X	X			X	X		X			X					X	X
Monumentos Nacionais	X																								X
Esgotos/Resíduos	X										X			X	X	X		X					X	X	X
Telecomunicações	X	X	X	X	X	X	X	X	X	X	X	X	X		X	X		X	X	X	X	X		X	X
Transportes/Logística	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X		X	X	X	X	X	X
Distribuição de Água	X		X		X	X	X	X	X		X	X		X	X	X				X	X	X	X	X	X

Fonte: Sá, 2017

No plano internacional, a União Européia consolidou essa perspectiva por meio da Diretiva (UE) 2022/2557 — *Critical Entities Resilience Directive* (*CER*) —, que estabelece obrigações aos Estados-membros. Incluiu a identificação de entidades críticas, a avaliação de riscos sistêmicos e o fortalecimento da resiliência em serviços essenciais frente a ameaças físicas e cibernéticas (UE, 2022). Isso amplia o escopo de proteção para além de ameaças deliberadas, incorporando riscos naturais, tecnológicos e híbridos, e exigindo avaliações integradas de risco e cooperação público-privada. De modo convergente, o DHS (United States, 2013) estrutura a proteção às ICs com base em gestão de riscos e parcerias multissetoriais, reconhecendo que a continuidade dos serviços depende da integração entre segurança física e cibernética.

Como elemento central dessa metodologia de proteção está o conceito de interdependência sistêmica, que se manifesta em quatro dimensões: física (dependência material entre setores), cibernética (integração por redes digitais), geográfica (proximidade territorial com vulnerabilidades compartilhadas) e lógica (vínculos funcionais ou financeiros) de acordo com o DHS (United States, 2018), em seu *National Infrastructure Protection Plan*. Essas interdependências produzem efeitos em cascata, evidenciando que a IC não se resume a "prédios e máquinas", mas constitui uma rede dinâmica de fluxos essenciais.

A resiliência de infraestruturas críticas depende diretamente do apoio mútuo entre essas infraestruturas, implicando em que a interdependência tenha um impacto decisivo na capacidade do sistema se recuperar, pois normalmente existem relações de apoio mútuo entre elas (Wang et al., 2021).

No Brasil, a proteção das ICs é incorporada pela Estratégia Nacional de Segurança de Infraestruturas Críticas (ENSIC), aprovada pelo Decreto nº 10.569, de 9 de dezembro de

2020 (Brasil, 2020a), e pelo Plano Nacional de Segurança de Infraestruturas Críticas (Plansic), instituído pelo Decreto nº 11.200, de 15 de setembro de 2022 (Brasil, 2022a), ambos editados pela Presidência da República. A coordenação compete ao Gabinete de Segurança Institucional (GSI), que articula setores estratégicos como energia, transportes, recursos hídricos e finanças. Embora o país acompanhe a tendência global de securitização desses ativos, enfrenta desafios estruturais relevantes, como obsolescência tecnológica e dispersão geográfica, que complexificam a governança e exigem fortalecimento contínuo da resiliência sistêmica.

2.4 A CONEXÃO ENTRE CRIME ORGANIZADO E AMEAÇAS HÍBRIDAS

A conexão entre crime organizado e ameaças híbridas revela a transformação qualitativa da natureza dos riscos que incidem sobre as infraestruturas críticas. Tradicionalmente vinculadas a crimes de natureza econômica — como tráfico de drogas, contrabando e lavagem de capitais —, as organizações criminosas contemporâneas passaram por um processo de reconfiguração estrutural, assumindo características de redes transnacionais altamente adaptativas.

Atualmente, tais grupos combinam violência armada, infiltração e corrupção institucional, diversificação de mercados ilícitos e emprego de capacidades tecnológicas avançadas, incluindo operações cibernéticas sofisticadas, ampliando significativamente seu potencial de impacto sistêmico (UNODC, 2023; Europol, 2021).

Pestana (2024) pontua que as ameaças híbridas são ações coordenadas e sincronizadas com o fim de explorar vulnerabilidades em ataques a valores fundamentais e liberdades dos estados. Essas ações advém de atores híbridos, os quais exploram desastres naturais ou atos de sabotagem para questionar a credibilidade dos regimes democráticos. O termo “híbrida” vem sendo substituído por “assimétrica”, por se tratarem de ameaças variadas e imprevisíveis, de grande intensidade e com utilização de armamentos incomuns, especialmente quando envolve a criminalidade organizada e o terrorismo (Miovska, 2022).

No plano internacional, esse fenômeno é descrito pelo conceito de *Crime-Terror Nexus*, entendido como a convergência operacional, logística e financeira entre organizações criminosas e grupos terroristas, seja por meio de cooperação estratégica, compartilhamento de rotas e recursos, ou pela hibridização de métodos e objetivos (UNODC, 2019; Europol, 2022). Embora não se confundam conceitualmente, ambos compartilham métodos, redes logísticas e estratégias de financiamento, aproximando-se no uso instrumental da violência e da intimidação para obtenção de poder político ou econômico.

A evolução das Organizações Criminosas Transnacionais (OCTs) demonstra que tais grupos passaram a explorar vulnerabilidades estruturais dos sistemas modernos. Em vez de apenas operar à margem do Estado, essas organizações passaram a incidir diretamente sobre infraestruturas estratégicas, mobilizando instrumentos associados à chamada “guerra híbrida”. Tais ataques englobam sabotagem física, ataques cibernéticos, coação territorial e exploração de vulnerabilidades institucionais, com potencial de gerar efeitos sistêmicos sobre a continuidade de serviços essenciais, conforme reconhecido na PNSIC, do Gabinete de Segurança Institucional da Presidência da República (GSI) (Brasil, 2018), e na Estratégia Nacional de Defesa, do Ministério da Defesa (Brasil, 2020b).

Os grupos criminosos utilizam como estratégias ataques cibernéticos a redes elétricas, bloqueio de sistemas hospitalares, sabotagem logística e campanhas de ransomware voltadas à extorsão de empresas e governos. No contexto brasileiro, tais ameaças são reconhecidas oficialmente pela Agência Nacional de Segurança Cibernética — no âmbito da

Gabinete de Segurança Institucional — e pelo Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov), que registram o crescimento de incidentes contra órgãos públicos e infraestruturas estratégicas. Esses grupos têm como objetivo não apenas o lucro imediato, mas também a criação de instabilidade sistêmica que aumente a capacidade de chantagem econômica e amplie zonas de influência. Nesse contexto, a infraestrutura crítica — compreendida como rede de serviços vitais e fluxos digitais — torna-se alvo estratégico, pois sua interrupção gera impactos amplificados, produz efeitos em cascata entre setores interdependentes e pressiona autoridades públicas a responder sob condições de elevada vulnerabilidade (CTIR Gov, Relatórios de Incidentes Cibernéticos).

No Brasil, essa dinâmica assume contornos próprios. Facções como o Primeiro Comando da Capital (PCC) e o Comando Vermelho (CV) passaram por um processo de sofisticação organizacional que as deslocou da condição de redes predominantemente voltadas ao varejo de drogas para estruturas de governança criminal territorial. A partir disso, exercem controle social armado, promovem a regulação de mercados ilícitos e influenciam sobre dinâmicas econômicas locais, conforme apontado no Relatório Nacional sobre Crime Organizado, do Ministério da Justiça e Segurança Pública (Brasil, 2022b), e no Anuário Brasileiro de Segurança Pública 2023, do Fórum Brasileiro de Segurança Pública (FBSP, 2023).

Em diversas periferias urbanas, esses grupos exercem controle sobre serviços essenciais, como provedores clandestinos de internet, distribuição informal de gás e transporte alternativo, configurando uma espécie de “insurgência criminal” urbana. A atuação vai além da economia ilícita tradicional, envolvendo regulação de mercados locais, imposição de normas coercitivas e captura de fluxos financeiros.

A conexão entre crime organizado e ameaças híbridas reside na estratégia de substituição funcional do Estado em determinados territórios, mediante o exercício de controle social armado, regulação paralela de mercados e imposição de normas próprias. Nesse contexto, o objetivo dessas organizações não se limita à comercialização de entorpecentes, mas à consolidação de poder político-econômico por meio do domínio de infraestruturas locais — formais ou informais — e da influência sobre serviços essenciais e atividades econômicas estratégicas (Brasil, 2022b; FBSP, 2023).

Ao controlar serviços essenciais, as organizações criminosas ampliam sua legitimidade coercitiva, fortalecem mecanismos de lavagem de dinheiro e consolidam influência social. Nesse cenário, a ameaça às infraestruturas críticas não decorre apenas de sabotagem externa, mas da infiltração e captura gradual de sistemas essenciais por atores criminais que operam segundo lógicas híbridas de poder, mercado e coerção.

2.5. GOVERNANÇA, PROTEÇÃO E O PARADIGMA DA RESILIÊNCIA

A governança das infraestruturas críticas estrutura-se como o arranjo institucional, normativo e operacional por meio do qual Estado e setor privado coordenam decisões, compartilham informações e gerenciam riscos com vistas à proteção e à continuidade de serviços essenciais, conforme delineado na PNSIC (Brasil, 2018), do Gabinete de Segurança Institucional da Presidência da República.

No paradigma contemporâneo, proteção não se confunde com invulnerabilidade, mas com a capacidade sistêmica de antecipar, absorver, adaptar-se e recuperar-se de disrupções, em consonância com a abordagem de resiliência prevista na Estratégia Nacional de Defesa, do Ministério da Defesa (Brasil, 2020b). Nesse contexto, consolida-se o paradigma da resiliência, que desloca o foco da “proteção total” — tecnicamente inviável em ambientes

complexos e interconectados — para a manutenção da continuidade operacional e da rápida recuperação funcional após incidentes.

Ao tratar da proteção e do paradigma da resiliência, Jungwirth (2023) destaca o papel das camadas locais na proteção das ICs. Para o autor, o processo se inicia com as comunidades, as quais possuem um sentimento de unidade e pertencimento. Em segundo lugar, o autor elenca a administração local, responsável pelos principais serviços de uso imediato das populações. Na sequência, tem-se a governança em nível estatal, que possui importantes vetores de resiliência, tais como o parlamento, a administração federal, tribunais e as forças armadas.

No plano internacional, o conceito de Resiliência Organizacional encontra referência normativa na International Organization for Standardization, por meio da norma ISO 22316:2017 — *Security and resilience — Organizational resilience — Principles and attributes*, que define a resiliência como um atributo estratégico incorporado à cultura institucional, à estrutura de governança, à gestão de riscos e à capacidade adaptativa das organizações (ISO, 2017).

Nesse sentido, a governança multissetorial torna-se elemento central, reconhecendo que a maior parte das infraestruturas críticas é operada por empresas privadas. Nos Estados Unidos, sob coordenação do DHS, consolidaram-se modelos estruturados de parceria público-privada para a proteção de infraestruturas críticas, especialmente a partir do *National Infrastructure Protection Plan* (NIPP), que estabelece a integração entre governo federal e operadores privados como eixo central da gestão de riscos (United States, 2013).

Setores como energia, telecomunicações e finanças compartilham inteligência de ameaças por meio dos *Information Sharing and Analysis Centers* (ISACs), conforme sistematizado pela *Cybersecurity and Infrastructure Security Agency* (CISA, 2023). De modo semelhante, a União Européia instituiu, por meio da *Directive (EU) 2022/2557 on the resilience of critical entities* (CER *Directive*), um modelo cooperativo que impõe aos Estados-membros a adoção de mecanismos de coordenação entre autoridades públicas e operadores privados, reconhecendo que a proteção eficaz de serviços essenciais depende da circulação contínua de informações estratégicas sobre riscos emergentes (EU, 2022).

No Brasil, essa agenda é incorporada pela Política Nacional de Cibersegurança (PNCiber) instituída pelo Presidência da República por meio do Decreto nº 11.856, de 26 de dezembro de 2023 (Brasil, 2023) e por fóruns de governança que buscam integrar órgãos de segurança pública, defesa, agências reguladoras e operadores privados. Contudo, a resposta institucional enfrenta desafios estruturais, notadamente a fragmentação de competências entre polícias federais e estaduais, ministérios setoriais e entidades regulatórias. Essa dispersão decisória dificulta a coordenação em incidentes que afetam serviços essenciais, especialmente quando envolvem dimensões simultaneamente físicas e cibernéticas.

Assim, a consolidação do paradigma da resiliência no Brasil depende menos da construção de barreiras físicas e mais da edificação de uma governança de inteligência integrada, capaz de articular o setor privado — proprietário ou operador das infraestruturas — e o setor público — responsável pela repressão criminal e pela segurança nacional. A eficácia da proteção, nesse modelo, reside na capacidade de cooperação, compartilhamento de informações e tomada de decisão coordenada diante de ameaças complexas e híbridas.

3 METODOLOGIA DO TRABALHO

Este estudo adota abordagem qualitativa, de natureza exploratória e descritiva, fundamentada em uma revisão integrativa da literatura, complementada por análise

documental de legislações, políticas públicas e documentos institucionais nacionais e internacionais. A opção pela revisão integrativa justifica-se por sua adequação à análise de fenômenos complexos e multidimensionais, como a proteção de infraestruturas críticas frente à atuação de organizações criminosas, permitindo a síntese crítica de estudos com diferentes enfoques teóricos, metodológicos e empíricos.

A revisão seguiu um protocolo estruturado em etapas sequenciais, compreendendo: definição do problema de pesquisa; seleção das bases de dados; formulação das estratégias de busca; aplicação de critérios de inclusão e exclusão; leitura exploratória, analítica e interpretativa dos estudos selecionados; e organização dos achados em dimensões analíticas. A questão orientadora da revisão consistiu em identificar como a literatura acadêmica e institucional aborda os ataques e ameaças de organizações criminosas às infraestruturas críticas, especialmente os serviços essenciais, bem como os modelos de proteção, vulnerabilidades e estratégias de resposta adotados no Brasil e no contexto internacional.

As buscas foram realizadas nas bases Scopus, Web of Science, SciELO e Google Scholar, utilizando descritores em português e inglês combinados por operadores booleanos. A string principal de busca incluiu os termos: (“infraestruturas críticas” OR “infraestrutura crítica” OR “serviços essenciais” OR “critical infrastructure” OR “essential services”) AND (“crime organizado” OR “organizações criminosas” OR “organized crime” OR “criminal organizations” OR “hybrid threats”) AND (“segurança” OR “proteção” OR “resiliência” OR “governança” OR “security” OR “resilience” OR “governance”). Em razão das particularidades técnicas de cada base, foram realizadas variações pontuais na *string*, com ajustes de campos de busca e simplificação de termos, preservando-se a coerência conceitual. Os resultados obtidos em cada base constam no Quadro 2.

Quadro 2 - Total de artigos recuperados por base de dados

Base de dados / Fonte de busca	**Tipo de documentos identificados**	**Total de documentos identificados**	**Observações metodológicas**
SciELO	Artigos de periódicos científicos	132	Prioridade para produção científica brasileira em segurança pública, criminologia e estudos de fronteira.
Scopus	Artigos de periódicos científicos	63	Utilizado para acesso a periódicos científicos e obras acadêmicas especializadas considerando a temática do trabalho.
Web of Science	Artigos de periódicos científicos	16	Utilizado para acesso a periódicos científicos e obras acadêmicas especializadas considerando a temática do trabalho.
Google Scholar	Teses, Dissertações e Monografias	3	Utilizado para acesso a periódicos científicos e obras acadêmicas especializadas considerando a temática do trabalho.
Período das buscas: 01 de outubro de 2025 a 15 de outubro de 2025.			

Fonte**:** elaborado pelos autores

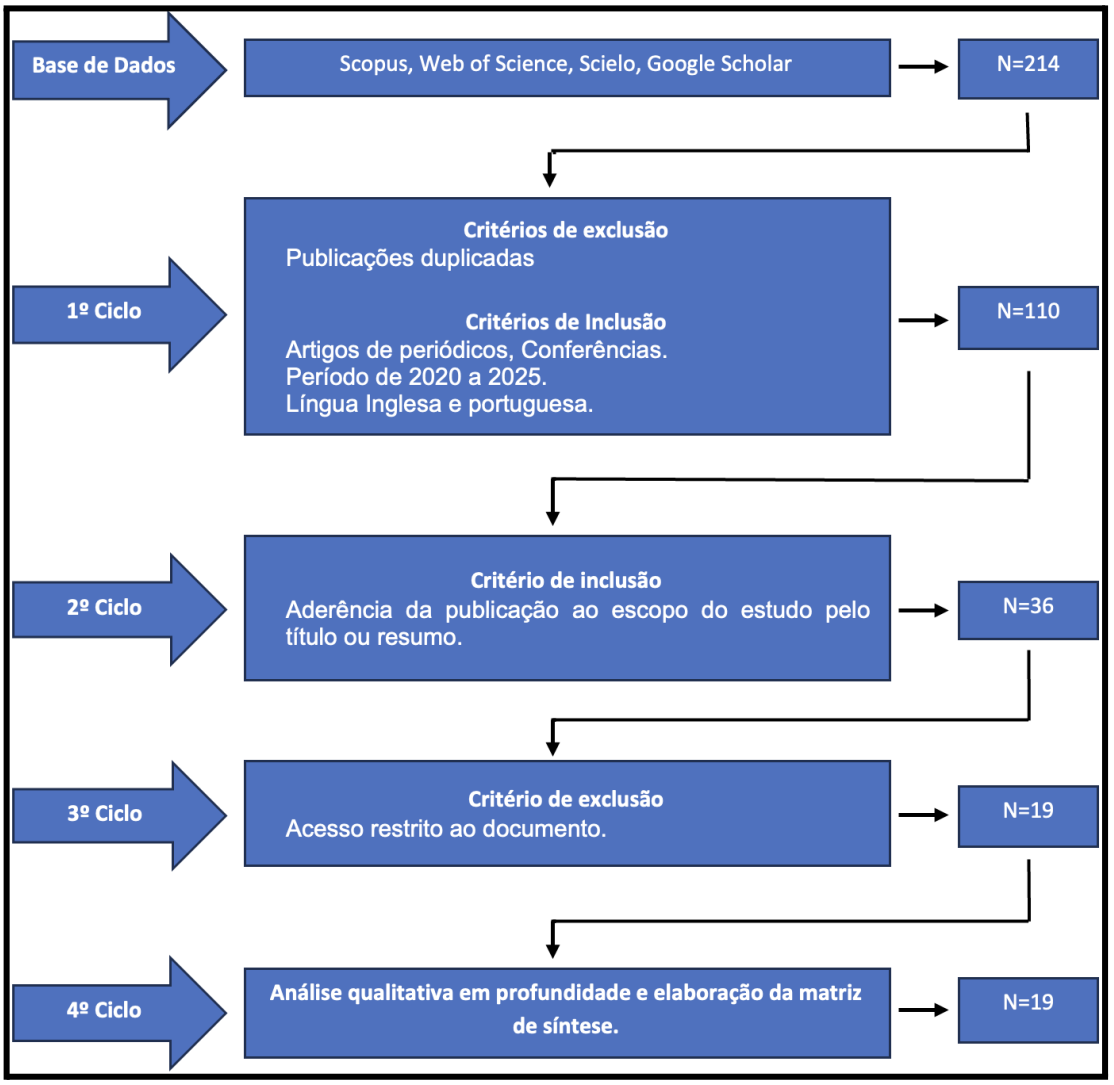
A aplicação da estratégia de busca, realizada no período de 01 de outubro de 2025 a 15 de outubro de 2025, resultou em um conjunto inicial de estudos distribuídos entre as bases consultadas totalizando 214 artigos. Após a remoção de duplicados e definição do contexto dos artigos por meio dos critérios de inclusão, 110 artigos permaneceram. Na sequência

procedeu-se à triagem por meio da leitura de títulos e resumos, finalizando com a seleção de 19 artigos. Com base nesses artigos, realizou-se a leitura integral dos textos elegíveis. Foram incluídas publicações com aderência temática direta ao objeto de estudo, disponíveis integralmente em português, inglês ou espanhol, abrangendo artigos científicos, livros, capítulos e documentos institucionais oficiais.

Excluíram-se trabalhos duplicados, estudos sem acesso ao texto completo, produções meramente opinativas e pesquisas exclusivamente técnicas dissociadas das dimensões de segurança, governança ou criminalidade organizada. Ao final do processo, o corpus analítico foi composto por 19 estudos que subsidiaram a análise desenvolvida na Seção 4. Cabe mencionar que, para subsidiar a análise, foram definidas algumas dimensões visando a construção de uma matriz de síntese da pesquisa, disponível no Apêndice A.

O percurso metodológico adotado é sintetizado em um fluxograma (Figura 1), que representa de forma esquemática todas as etapas da revisão integrativa, desde a identificação inicial dos estudos até a seleção final, indicando os quantitativos obtidos em cada fase do processo. Esse procedimento assegura transparência, reprodutibilidade e coerência entre os objetivos da pesquisa, o método empregado e as conclusões alcançadas.

Figura 1 - Fluxograma indicando o percursos metodológico



Fonte: elaborado pelos autores

4 ANÁLISE E DISCUSSÃO DOS RESULTADOS

Esta seção analisa a matriz de síntese gerada na etapa anterior de modo a subsidiar a discussão de cada uma das dimensões visando analisar como estas impactam na temática central do trabalho.

4.1 TIPO DE ESTUDO E METODOLOGIA PRINCIPAL

O presente estudo possui escopo essencialmente qualitativo, partindo de uma revisão integrativa acerca do tema, com ênfase na literatura nacional e internacional. De plano notou-se, comparativamente, uma deficiência na literatura nacional a respeito da temática, a qual, via de regra, fica adstrita a trabalhos acadêmicos militares e/ou policiais.

No restante do mundo há uma produção acadêmica majoritariamente voltada ao ambiente cibernético-corporativo, sob a tutela de quem se encontra maior parte da administração de infraestruturas críticas no mundo; ambiente aquele marcado pela integração de objetos físicos e infraestruturas à rede mundial de computadores.

No âmbito nacional destacam-se os trabalhos de Nonato e Pinho (2021) que buscaram traçar o estado atual da proteção de infraestruturas críticas no Brasil, sugerindo sua integração ao Sistema Militar de Defesa Cibernética como forma de possível mitigação dos riscos. Já Ferreira (2017), apesar de uma abordagem qualitativa, possui foco maior no estudo comparativo entre diversos critérios adotados no mundo, propondo conceitos metodológicos para a identificação e caracterização de infraestruturas críticas.

No trabalho de Oliveira, Andrade e Monteiro (2022) os autores utilizaram uma matriz SWOT para analisar a migração da gestão da infraestrutura aeroportuária da Empresa Brasileira de Infraestrutura Aeroportuária - Infraero para o setor privado, considerando, em especial, seu afastamento do Sistema Brasileiro de Inteligência – SISBIN. As conclusões são de extrema relevância pois demonstram a necessidade de os atores privados integrarem e cooperarem com o sistema de inteligência estatal.

Internacionalmente citam-se os trabalhos produzidos por Govea, Gaibor-Naranjo e Villegas-Ch (2024) e Lozano *et al*. (2023). O foco maior reside em estudos experimentais quantitativos com o uso de ML, com uma abordagem mais voltada para a Ciência da Computação e Engenharia, explorando soluções, em especial tecnológicas, para enfrentar os desafios das ameaças cibernéticas a infraestruturas críticas.

Identificou-se também que uma parte da literatura está direcionada para uma abordagem em estudos de natureza conceitual e análise de cenário, sendo eles: Nonato e Pinho (2021), Inácio e Silva (2023), Badin *et al*. (2023), Guterres (2016), Ferreira (2017) e Gülcan e Erginer (2023). Dentro dessa abordagem teórico-qualitativa é possível também distinguir os autores que dedicam seus esforços na proposição de conceitos e cenários de futuras ameaças (Ferreira, 2017; Gülcan e Erginer, 2023).

Destaca-se na análise realizada, o artigo de Siqueira, Nascimento e Moraes (2022), único estudo que utilizou trabalho de campo direto, incluindo entrevistas e observação, para gerar dados primários sobre governança criminal, distanciando-se da análise puramente documental. Por sua vez, Ramos, Rocha e Zahreddine (2021), propôs uma análise híbrida (qualitativa e quantitativa), utilizando uma técnica específica de análise de conteúdo sobre um objeto fechado, as declarações de cúpula dos BRICS.

Do ponto de vista metodológico, identificou-se uma dicotomia metodológica entre os blocos de autores: de um lado, as Ciências Sociais e Jurídicas utilizando a revisão documental

e ensaios teóricos; e, de outro lado, as Ciências Computacionais focadas em testes experimentais e revisão de padrões técnicos.

4.2 FOCO GEOPOLÍTICO E NÍVEL DE ANÁLISE

Para esta dimensão, os artigos analisados concentram-se especialmente no nível estatal brasileiro, os quais tratam o sistema de proteção de infraestruturas críticas como uma questão de soberania interna e defesa nacional. A maior parte da produção acadêmica acerca da temática em estudo é decorrente de programas institucionais de capacitação, em especial nas áreas de estudos militares e de segurança pública.

Em consonância com o fenômeno da Internet das Coisas (do inglês *Internet of Things* - IoT) e a crescente integração de objetos e infraestruturas ao mundo cibernético, Nonato e Pinho (2021) apontam um aumento de ataques cibernéticos a infraestruturas críticas pelo mundo. Propõem para o cenário brasileiro uma integração dos sistemas de proteção dessas infraestruturas com o Sistema Militar de Defesa Cibernética (SMDC), já existente, que possui como órgão central o Comando de Defesa Cibernética do Exército Brasileiro.

Por sua vez, Inácio e Silva (2023), promoveram um estudo com recorte temporal específico, tratando especialmente da geopolítica militar brasileira no Governo de Jair Messias Bolsonaro, considerando a segurança das infraestruturas críticas nacionais e a grande participação de militares no governo civil. Analisando as políticas públicas do período e os discursos proferidos por militares ocupantes de cargos civis estratégicos, os autores concluem que o controle político sobre o território nacional, em especial nos períodos de militarização da política, passa pela proteção das infraestruturas críticas, perfazendo-se em objetivo estratégico dos militares.

Não por outro motivo, os marcos normativos-legais brasileiros, em especial a PNSIC (Brasil, 2018); a Estratégia Nacional de Segurança de Infraestruturas Críticas (Brasil, 2020a) e o Plano Nacional de Segurança de Infraestruturas Críticas (Brasil, 2022a), são frutos desse período em que houve alta ocupação de militares nos postos civis estratégicos, caracterizado também pelo GSI como “Ministério dos Ministérios”, chefiado por um militar. Analisando também o cenário regulatório brasileiro, Guterres (2016) trouxe estudo indicando que a proteção e regulação do sistema de proteção de infraestruturas críticas tem íntima relação com a ocorrência de eventos de grande impacto na sociedade e a busca por minimização de riscos e incertezas relacionados.

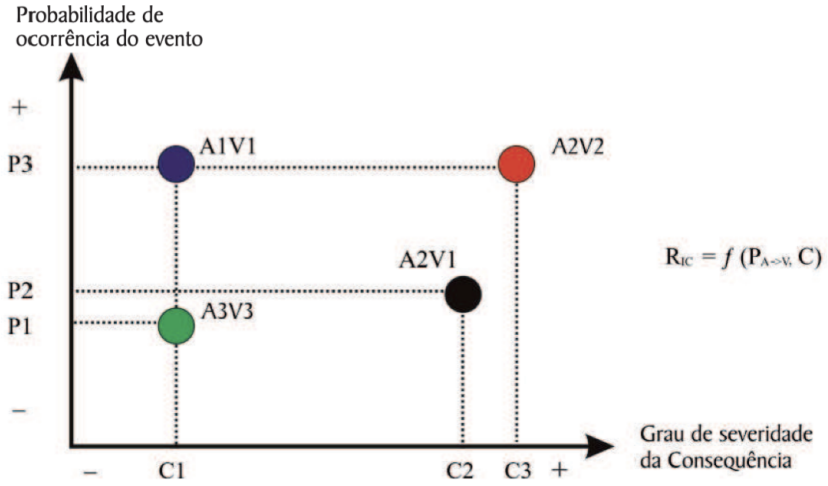
No Brasil, da mesma forma, os Jogos Olímpicos (Rio 2016) e a Copa do Mundo Fifa (Brasil 2014) influenciaram diretamente o processo de maturação regulatória no Brasil. Importante contribuição foi apresentada por Miranda Filho (2012), em estudo onde divide o processo de proteção das infraestruturas críticas em quatro fases: identificação, prevenção, resiliência e retroalimentação; indicando em quais pontos a inteligência de estado pode contribuir em cada etapa.

O processo é apresentado de forma cíclica, por meio de retroalimentação das fases de identificação, prevenção e resiliência. A fase de identificação dos riscos e das infraestruturas críticas ocorre por meio de grupos de estudo, em regra compostos por órgãos públicos, agências reguladoras, especialistas, dentre outros. Na etapa de prevenção ocorre o entendimento do risco no contexto de proteção das infraestruturas críticas, aplicando-se equações de análise de probabilidades da ameaça visando explorar uma vulnerabilidade, acarretando consequências danosas aos usuários.

Miranda Filho (2012) acrescenta o mapeamento de risco de uma IC, no qual a avaliação do risco pode ser representada por um gráfico de probabilidade X consequências

(Figura 2). Cada ponto representa uma ameaça que pode explorar uma vulnerabilidade; e, para cada ponto há uma probabilidade de ocorrência (eixo Y) e um grau de severidade da consequência (eixo X). O risco (RIC), por sua vez, é a função da probabilidade (P) de uma fonte de ameaça explorar uma vulnerabilidade (A -> V), acarretando consequências danosas (C).

Figura 2: Mapeamento de risco de uma infraestrutura crítica



Fonte: Miranda Filho (2012)

Identificados e classificados os riscos e probabilidades, a etapa da resiliência consiste na implementação de medidas voltadas a mitigar os efeitos do sinistro, reagir ao evento causador e restabelecer o pleno funcionamento da infraestrutura. O autor defende que o Sistema de Inteligência (SI), formado por todos os órgãos que integram o Sistema de Inteligência Brasileiro (SIB), possui capacidade técnica e administrativa para cooperar em todas as etapas. Tal visão é essencial, pois o SI possui fragmentação e capacidade operativa de contribuir de sobremaneira ao fortalecimento do Sistema de Proteção de Infraestruturas Críticas, em especial tratando-se de ataques promovidos por Organizações Criminosas, as quais também são objetos de estudos e análises de inteligência.

No cenário mundial, o trabalho de Guterres (2016) aborda, em especial quanto aos investimentos externos, que as infraestruturas críticas de um país sejam consideradas na implementação dos Instrumentos de Avaliação de Investimento Externos (IAIEs). Após a análise, o estudo busca identificar se o Brasil, por ocasião da implementação de investimentos externos em território nacional, considera tal critério no processo decisório. Países como África do Sul, China, Coreia do Sul, Japão, Alemanha, Austrália, Canadá e Estados Unidos da América consideram, ainda que de maneira genérica, as infraestruturas críticas no processo de investimentos externos em outros países; havendo preocupação com a participação de capital externo em infraestruturas críticas nacionais.

O estudo conclui que o Brasil ainda é tímido no sentido de proteger infraestruturas estratégicas da participação excessiva de capital estrangeiro, o que poderia representar uma vulnerabilidade do país em casos de ataques externos. Acrescenta-se o fato de que, no Brasil, o processo de investimentos em infraestruturas críticas passa por um processo de "liberalização, flexibilização e facilitação de acesso da iniciativa privada, seja ela de origem nacional ou estrangeira".

Wendt (2011), traçando um panorama do cenário mundial, apresenta a inteligência cibernética como forma de subsidiar as decisões governamentais ou não na prevenção de incidentes cibernéticos, os quais cada dia mais tem relação e interconectividade com infraestruturas críticas. O autor apresenta uma análise demonstrando a crescente preocupação com a criminalidade virtual, escalonando essa atuação desde o cibervandalismo, passando pelo crime cometido na internet, espionagem cibernética, terrorismo cibernético até a guerra cibernética. Conclui indicando que o cenário brasileiro ainda é muito alarmante, com uma grande insegurança cibernética, em especial pela existência de diversos atores privados em serviços essenciais, os quais não possuem controle estatal de segurança orgânica, especialmente cibernética.

A partir de uma análise em foco local, Siqueira, Nascimento e Moraes (2022) realizaram estudo comparativo da governança criminal entre Manaus/AM e Fortaleza/CE. O autor aborda uma análise do que chama de governança criminal, que envolve a dominação de territórios, o trato com a população, a disponibilização de serviços e, até mesmo, a relação com as estruturas estatais. Conclui-se que a situação carcerária brasileira é uma espécie de nascedouro e catalisador das organizações criminosas e/ou facções que realizarão a dominação de territórios fora das penitenciárias. Essas organizações desenvolvem verdadeira governança criminal como forma de se manterem proeminentes e com legitimidade perante as populações locais.

No âmbito dos blocos internacionais, ao analisar a agenda de segurança dos BRICS, Ramos, Rocha e Zahreddine (2021) evidenciaram que o bloco, originalmente criado em decorrência de mútuos interesses econômicos, avança para temáticas envolvendo a segurança internacional. Por exemplo, na cúpula de Delhi teve como tema central a contribuição do BRICS para a Estabilidade Global, Segurança e Prosperidade. O estudo demonstrou, a partir da análise das cúpulas do grupo uma crescente preocupação com a segurança cibernética e proteção das infraestruturas críticas, especialmente em face do terrorismo. Em Goa (2016) foi estabelecido o BRICS *Roadmap of Practical Cooperation on Ensuring Security in the Use of* ICTs, onde há previsão da possibilidade de compartilhamento de informações entre os integrantes do grupo, acerca de ciberameaças, visando mitigar potenciais riscos a infraestruturas críticas.

Já no trabalho de Gülcan *et al.* (2023), no mesmo sentido, ao analisar a segurança de infraestruturas marítimas, defende a existência de estrutura intergovernamental de proteção marítima, estabelecendo, ao menos, uma doutrina de identificação de riscos e compartilhamento de informações. O estudo traz como marco o ataque de sabotagem às linhas de gás no Mar Báltico, ocorridas em 2022, construídas para transpor gás da Rússia à Alemanha. O estudo realiza um comparativo dos modelos de proteção de infraestruturas críticas nos países e nos blocos de países que adotam regras comuns. Aponta também a importância de que essa proteção internacional recaia sobre os cabos submarinos de tráfego de dados.

No Brasil, os principais *hubs* de comunicação se encontram nos estados do Ceará, São Paulo e Rio de Janeiro. Tais infraestruturas representam dupla importância, pois além de serem propriamente uma infraestrutura crítica, um ataque à sua higidez pode comprometer outras infraestruturas de dependam de comunicações de dados / cibernéticas. Udeanu (2015), ao tratar do sistema de proteção de infraestruturas críticas da Romênia, ressalta a importância que esse processo, que é dinâmico, deve ir de encontro às diretrizes dos blocos de interesse regional, União Europeia e Organização do Tratado do Atlântico Norte (OTAN).

No âmbito dos estudos focados em engenharia e ciência da computação, nota-se uma visão mais global da abordagem, extrapolando o foco geopolítico anteriormente visto. Essa

visão considera as fronteiras geográficas irrelevantes no contexto da tecnologia e proteção dos ambientes cibernéticos.

Nesse sentido, Daousis *et al*. (2024), apresenta a evolução da implementação de redes de comunicação nos mais variados espectros das infraestruturas críticas. O autor ressalta a necessidade de que a comunidade (não países ou blocos regionais) preocupem-se em criar e aplicar protocolos de proteção e salvaguarda do ambiente no qual as infraestruturas estão baseadas ou dependem essencialmente. Já Govea, Gaibor-Naranjo e Villegas-Ch (2024), por sua vez, defendem em seu estudo a utilização de *blockchain* como forma de ciber-resiliência aplicável a infraestruturas críticas. Os autores consideram que a descentralização característica do *blockchain* possui maior capacidade de promover a proteção e transparência necessárias à salvaguarda do ambiente cibernético. Há, portanto, uma visão globalista da tecnologia, a qual, de certa forma, busca o afastamento de entidades governamentais na proteção às infraestruturas ligadas ao ambiente cibernético.

Em abordagem similar, Lozano, Llopis e Domingo (2023) defendem a utilização de uma abordagem de ML como forma de identificar e antecipar ameaças a infraestruturas críticas. Os autores abordam a grande capacidade de tais soluções, especialmente por meio de AI, para aprender padrões indicativos de ameaças, auxiliando a análise de dados massivos decorrentes de infraestruturas ligadas cada vez mais a um mundo hiper conectado.

A literatura que integrou a revisão da literatura passou por abordagens locais, nacionais, regionais, intercontinentais e globais. Identificou-se que análises com maior escopo geopolítico, tendem a estudar o fenômeno sob a ótica de regiões geográficas ou de países e/ou blocos de países. Já os estudos voltados à engenharia e ciência da computação, possuem uma visão mais global do fenômeno, entendendo que sua abrangência extrapola a formação de estados e blocos internacionais. Na proposição de soluções, a abordagem também busca o fomento de soluções da própria comunidade de tecnologia, adotando soluções próprias na mitigação de ameaças, como o blockchain e machine learning.

Em que pese os diferentes escopos apresentados, a relação intrínseca entre cibersegurança e proteção das infraestruturas críticas é praticamente onipresente. A IoT e a hiperconexão entre infraestruturas e objetos, torna o ambiente cibernético o cenário no qual a mitigação de ameaças deve se concentrar. Outro aspecto comum aos estudos é que não há um ambiente seguro relacionado às infraestruturas críticas em todo mundo. O desafio de estados e blocos regionais na proteção das infraestruturas essenciais de seus povos se encontra na agenda interna e internacional dos governos, os quais atualmente tentam compreender e se integrar a um ambiente que ainda lhes é estranho, criado, por essência, por corporações privadas de tecnologia.

No âmbito da presente revisão, por sua vez, é relevante ressaltar a natureza das organizações criminosas e/ou facções nacionais, as quais tendem a exercer dominação territorial, disputando espaço de legitimidade com o poder público. É comum no Brasil que, em regiões dominadas por grupos criminosos, serviços essenciais à população passem a ser fornecidos por eles, tais como internet, gás e transporte. Sob tal ótica, as infraestruturas críticas podem ser objeto de ataque por criminosos não só para desestabilizar o Estado, mas também para viabilizar uma prestação própria de serviços por criminosos, em busca de benefício econômico e de legitimidade perante a população.

4.3 ATORES CRIMINOSOS E ESTRUTURA ANALISADA

A literatura não trata os atores criminosos (organizações criminosas) de forma uniforme. Há uma variação clara entre trabalhos que descrevem esses atores de maneira

profunda, como organizações sociais complexas, e estudos que os apresentam apenas como categorias genéricas de ameaça. Essa diferença revela distintas formas de entender quem é o "inimigo" e qual nível de detalhamento é considerado relevante para a análise e para a formulação de políticas de defesa.

De um lado, alguns autores desenvolvem análises detalhadas sobre a estrutura e o funcionamento dos grupos criminosos. Siqueira, Nascimento e Moraes (2022) apresentam um exemplo central dessa abordagem, ao examinar facções criminosas brasileiras como organizações com regras próprias, hierarquias, normas internas e formas de controle territorial e prisional. Nessa perspectiva, o ator criminoso é visto como um coletivo organizado, capaz de planejar, adaptar estratégias e exercer governança sobre seus membros. Em contraste, trabalhos como os de Ferreira (2017) e Miranda Filho (2012) tendem a tratar os atores criminosos de forma mais genérica, apresentando-os como listas de riscos ou ameaças, sem aprofundar sua estrutura social ou organizacional.

Essa diferença também aparece na forma como a literatura aborda a governança criminal. Apenas uma parte reduzida dos estudos analisa com mais detalhe a organização interna de grupos como o Primeiro Comando da Capital (PCC), o Comando Vermelho (CV) ou a Família do Norte. Pesquisas como as de Siqueira, Nascimento e Moraes (2022) e de Oliveira, Andrade e Monteiro (2022) descrevem hierarquias, funções, normas internas e a capacidade desses grupos de exercer comando a partir do sistema prisional. Esses trabalhos demonstram que as facções funcionam como estruturas organizadas e relativamente estáveis. No entanto, a maioria dos estudos não entra nesse nível de detalhe e trata esses grupos como unidades homogêneas.

Outro conjunto de trabalhos define os atores não pela sua estrutura interna, mas pela sua posição no cenário internacional. Nesses casos, os autores diferenciam atores estatais e não estatais ou falam em ameaças híbridas, associando-as a interesses geopolíticos. Estudos como os de Udeanu (2015), Ramos, Rocha e Zahreddine (2021) e Miranda Filho (2012), enfatizam a atuação de Estados, como Rússia e China, ou de redes transnacionais ligadas ao terrorismo e ao tráfico. O foco está mais na motivação política ou estratégica do que na organização concreta desses atores.

Há também uma parte da literatura que prefere classificar os atores por meio de categorias amplas, baseadas em motivações ou tipos de ação. Autores como Wendt (2011), Ferreira (2017) e Ramos Junior (2024) utilizam classificações como hacktivistas, criminosos cibernéticos, espiões ou terroristas. Essas tipologias ajudam a organizar o debate, mas não explicam como esses grupos se estruturam, tomam decisões ou se mantêm ao longo do tempo.

Em estudos voltados à defesa e à governança estatal, observa-se um deslocamento do foco do ator criminoso para o próprio Estado. Trabalhos como os de Nonato e Pinho (2021), Inácio e Silva (2023) e Ramos Junior (2024) analisam principalmente as instituições responsáveis pela defesa, como o GSI, as Forças Armadas e os órgãos de coordenação governamental. Nessa abordagem, a ameaça aparece como algo genérico e externo, sem que se discuta quem é, de fato, o ator que ataca. Essa invisibilidade do ator é ainda mais evidente em pesquisas de caráter técnico ou regulatório. Estudos sobre detecção de ataques por meio de ML, análise de vulnerabilidades ou regulação jurídica e econômica, como os de Lozano, Llopis e Domingo (2023), Guterres (2016), Badin *et al*. (2023) e Gülcan *et al.* (2023), concentram-se nos meios técnicos ou legais do ataque. O agente humano ou político envolvido nessas ações raramente é descrito ou problematizado.

Como consequência, a literatura mostra uma limitação importante para o desenvolvimento de ações de inteligência voltadas ao combate de ameaças. Quando não se compreende como os atores criminosos se organizam, quais são suas regras, objetivos e

formas de atuação, as estratégias de defesa tendem a ser reativas e pouco antecipatórias. A comparação entre a riqueza descritiva de autores como Siqueira, Nascimento e Moraes (2022) e as abordagens mais técnicas e abstratas, como as de Wendt (2011) e Lozano, Llopis e Domingo (2023), evidencia uma lacuna relevante: sem conhecer o ator, a capacidade de prever comportamentos e antecipar ameaças fica significativamente reduzida

4.4 MODUS OPERANDI E ALVOS DE INFRAESTRUTURA CRÍTICA

A literatura identifica dois tipos delineados de ataques às infraestruturas críticas, sendo ciberataques técnicos, com foco na utilização do ambiente cibernético como forma de inviabilizar o funcionamento da estrutura e ataques físicos, e sabotagem e/ou emprego de violência contra coisas.

Govea, Gaibor-Naranjo e Villegas-Ch (2024), propuseram a tecnologia de *blockchain* como forma de prevenir, resistir, recuperar-se e adaptar-se a ataques cibernéticos, garantindo a continuidade das operações e a proteção de dados e sistemas. O trabalho dos autores, que é essencialmente voltar aos ataques de natureza técnica, defende que essa modalidade de ataque aumentou exponencialmente nas últimas décadas em decorrência do fenômeno da IoT. No mesmo sentido, Lozano, Llopis e Domingo (2023), propõem o uso de AI como forma de potencializar a análise massiva de dados para identificar e antecipar as ameaças.

Sá (2017), apresentou em seu estudo uma série de ataques a infraestrutura críticas desencadeadas em face de ataques físicos e/ou de força bruta, como por exemplo os ataques aos oleodutos na Colômbia promovidos pelas Forças Armadas Revolucionárias da Colômbia (FARC), em especial nos anos de 2011 e 2013, utilizando explosivos. Em outro caso, em 2013, nos Estados Unidos da América, um indivíduo se infiltrou por um túnel subterrâneo e cortou as linhas de telefone próximas à subestação de energia Metcalf da Pacific Gas and Electric Company (PG&E), fato este sucedido por disparos provenientes de atiradores contra transformadores da subestação.

Ao longo das últimas décadas, contudo, nota-se uma atenção maior da literatura às modalidades cibernéticas de ataque, diante da diminuição dos atos de violência física contra as infraestruturas. Os vetores de ataques às camadas lógicas da infraestrutura são divididos pela literatura em ataques de *Jamming*, *Spoofing*, Negação de Serviço (DoS/DDoS) e *Ransonware*, além da possibilidade de inserção de dados falsos nos sistemas informáticos, como elenca Ramos Junior (2024).

Em alguns casos, como na modalidade de *Jamming*, o ataque pode ter natureza híbrida, por envolver o emprego de meios físicos bloqueadores de sinal, tendo como consequência a interrupção de um serviço de tecnologia. No cânone dos estudos de caso dos ataques cibernéticos que auxiliaram na identificação dessas modalidades, destacam-se o ataque cibernético ao Iran, ocorrido em 2010, chamado de *Stuxnet*, no qual cinco organizações iranianas foram infectadas, afetando a usina nuclear de *Natanz* (Nonato e Pinho, 2021). Relatam os autores que, em 2017, identificou-se um *malware* de origem russa, responsável por ataques de *ransonware*, criptografando os arquivos dos computadores atingidos. Os ataques voltaram-se contra hospitais, empresas de energia, aeroportos e bancos ucranianos.

No Brasil, em que pese a origem histórica estar relacionada aos ataques físicos contra infraestruturas de transporte público e de linhas de energia, recentemente ganhou repercussão o ataque cibernético ao Ministério da Saúde. Este ocorreu em dezembro de 2021, período da Pandemia do COVID-19, afetando a capacidade de monitorar e rastrear a propagação do vírus (Ramos Junior, 2024).

Ao tratar da Guerra de Quarta Geração, Silva (2015) ressalta a influência recebida de novas tecnologias e ideias, culminando na descentralização dos conflitos, tornando a sociedade civil, política e militar participantes diretos dos conflitos. Contudo, ainda é possível identificar a utilização de meios físicos para a implementação ou potencialização de ataques, caracterizando-os como ataques híbridos. Por fim, nota-se, na maior parte da literatura, especialmente aquela voltada aos aspectos geopolíticos relacionados às infraestruturas críticas, que a proteção a tais infraestruturas é tratada como uma abstração política ou legislativa, sem definir como os ataques ocorrem (Inácio e Silva, 2023; Ferreira, 2017; Guterres, 2016; Badin *et al*., 2020; Siqueira, Nascimento e Moraes, 2022; Ramos; Rocha; Zahreddine, 2021; e Gülcan *et al.*, 2023).

4.5 PRINCIPAIS ACHADOS E IMPACTO MEDIDO

A síntese dos principais achados revela que a proteção às Infraestruturas Críticas (ICs) permanece marcada por fragilidades estruturais, apesar do reconhecimento crescente de sua centralidade para a segurança nacional. A literatura indica que o desafio predominante não é apenas técnico, mas sobretudo institucional e político, relacionado à forma como a governança da defesa é concebida e operacionalizada.

Os estudos convergem, inicialmente, para o diagnóstico de uma governança fragmentada e incipiente. No Brasil, a ausência de uma estrutura nacional permanente e centralizadora compromete a coordenação interinstitucional e a continuidade das políticas públicas voltadas às ICs (Nonato e Pinho, 2021; Ramos Junior, 2024). Esse quadro não é exclusivo do contexto nacional: análises europeias demonstram que iniciativas de integração também enfrentam entraves decorrentes de soberania estatal, limitações legais e dificuldades de compartilhamento de informações sensíveis entre países e agências (Gülcan *et al.*, 2023). Como resultado, a proteção tende a assumir um caráter reativo e descontínuo, incapaz de responder adequadamente a ameaças sistêmicas (Oliveira; Andrade; Monteiro, 2022).

Outro conjunto relevante de achados aponta para vulnerabilidades estratégicas que vão além do ataque direto. A literatura evidencia que lacunas regulatórias e econômicas ampliam significativamente a exposição das ICs brasileiras. Destaca-se, nesse sentido, a inexistência de mecanismos eficazes de filtragem de investimentos estrangeiros em setores sensíveis, bem como a ausência de marcos jurídicos claros que viabilizem o compartilhamento de informações estratégicas entre o Estado e operadores privados (Badin, 2023; Wendt, 2011; Oliveira; Andrade; Monteiro, 2022). Essas fragilidades produzem um ambiente de risco estrutural, no qual a dependência do setor privado não é acompanhada por instrumentos adequados de controle e cooperação.

No que se refere ao modelo brasileiro de gestão, os estudos o caracterizam como militarizado e orientado a eventos. A política de proteção de ICs foi impulsionada, sobretudo, pela realização de grandes eventos internacionais, o que levou à rápida expansão de capacidades institucionais e operacionais (Guterres, 2016). Esse processo resultou em uma abordagem centralizada, ancorada no GSI e fortemente influenciada por uma lógica militar, com concentração territorial no eixo Sul–Sudeste (Inácio; Silva, 2023). Embora eficaz para cenários excepcionais, esse modelo mostrou limitações para a consolidação de uma governança permanente, civil e descentralizada.

Em contraste com essas fragilidades institucionais, os artigos de natureza técnica validam a eficácia de soluções tecnológicas e metodológicas específicas. Estudos empíricos demonstram que o uso de *Blockchain* contribui para a descentralização e integridade da gestão de dados críticos (Govea; Gaibor-Naranjo; Villegas-Ch, 2024), enquanto arquiteturas

avançadas de Redes Neurais Artificiais (do inglês *Artificial Neural Network* - ANN), possibilitam a detecção de anomalias em sistemas industriais (Lozano; Llopis; Domingo, 2023; Daousis, 2024). No plano metodológico, propostas integradas de análise de risco indicam que a combinação entre fatores técnicos, organizacionais e humanos é decisiva para elevar o nível de proteção das ICs (Ferreira, 2017).

Um achado dissonante emerge da literatura sociológica ao se contrastar a fragilidade estatal com a eficácia da governança criminal. Siqueira, Nascimento e Moraes (2022) demonstram que facções criminosas no Brasil desenvolveram formas sofisticadas de regulação social e econômica, capazes de organizar mercados, impor normas e mediar conflitos. Esse contraste evidencia uma assimetria organizacional relevante: enquanto o Estado enfrenta dificuldades para integrar suas estruturas de defesa, atores ilegais operam com maior coesão, previsibilidade e capilaridade territorial.

Por fim, consolida-se um consenso transversal de que a proteção baseada exclusivamente em perímetros físicos ou digitais é insuficiente. A literatura destaca que a segurança das ICs depende, cada vez mais, da capacidade de produzir Inteligência Cibernética prospectiva, orientada à antecipação de ameaças híbridas e à cooperação interagências e internacional (Wendt, 2011; Miranda Filho, 2012; Udeanu, 2015; Ramos; Rocha; Zahreddine, 2021). Assim, os achados indicam que o avanço real na proteção das ICs exige a superação de respostas fragmentadas, em favor de uma governança integrada, orientada por inteligência e sustentada por visão estratégica de longo prazo.

5 CONSIDERAÇÕES FINAIS

A análise desenvolvida ao longo deste estudo evidencia que a proteção das Infraestruturas Críticas (ICs) no Brasil enfrenta desafios que transcendem o domínio estritamente técnico, configurando-se, sobretudo, como um problema de governança pública, coordenação institucional e orientação estratégica do Estado. Embora a literatura reconheça avanços normativos relevantes, os achados indicam que o modelo brasileiro permanece marcado por fragmentação, descontinuidade e forte dependência de respostas reativas, o que compromete a capacidade nacional de antecipar e mitigar ameaças complexas e híbridas.

A principal implicação para as políticas públicas consiste na necessidade de reconfiguração estrutural da governança da proteção de ICs, mediante a criação de um órgão centralizador robusto, dotado de autoridade técnica, capacidade normativa e função permanente de coordenação interagências. As propostas de um Centro Nacional de Segurança Cibernética ou de uma Agência Nacional de Cibersegurança convergem para esse objetivo. Devem, assim, ser compreendidas como instrumentos de institucionalização de uma política de Estado, capaz de integrar esforços civis e militares, harmonizar ações setoriais e garantir continuidade estratégica para além de ciclos governamentais. A ausência de tal instância mantém o sistema ancorado em articulações difusas, limitando sua efetividade operacional.

Os resultados também demonstram que a proteção das ICs é intrinsecamente público-privada, exigindo que as políticas públicas reconheçam e institucionalizem essa condição. A centralidade de concessionárias e operadores privados na gestão de serviços essenciais, aliada à sua limitada integração ao Sistema Brasileiro de Inteligência (SISBIN), constitui uma vulnerabilidade estrutural. Assim, impõe-se a formulação de marcos legais e administrativos que viabilizem o compartilhamento seguro de informações estratégicas, estabeleçam deveres claros de cooperação e integrem a inteligência estatal à governança corporativa. Políticas que desconsideram esse eixo tendem a produzir um descompasso entre responsabilidade pública e controle efetivo.

No campo regulatório e econômico, o estudo identifica uma lacuna crítica relacionada à proteção da soberania estratégica. A inexistência de mecanismos específicos de triagem de investimentos estrangeiros em setores sensíveis expõe o país a riscos geopolíticos de longo prazo, associados à captura ou dependência de ativos essenciais. Desse modo, uma implicação direta para as políticas públicas é a necessidade de integrar a proteção das ICs às políticas de investimentos, incorporando critérios de segurança nacional, continuidade de serviços e resiliência estratégica nos processos decisórios do Estado.

No plano internacional, os achados indicam que a proteção das ICs não pode ser concebida exclusivamente no âmbito doméstico. Experiências da União Europeia e do BRICS demonstram que a cooperação supranacional é ao mesmo tempo necessária e limitada por interesses de soberania. Para o Brasil, isso implica reconhecer a proteção de infraestruturas críticas — especialmente cibernéticas e marítimas — como tema central da política externa e de defesa, demandando arranjos institucionais que permitam compartilhamento de informações, vigilância comum e coordenação estratégica, sem ignorar as assimetrias de interesse envolvidas.

No nível operacional, a literatura valida a incorporação de padrões técnicos e metodológicos específicos como parte integrante das políticas públicas de modernização. Metodologias ampliadas de identificação de ICs, protocolos industriais seguros e arquiteturas de defesa proativa baseadas em AI e *Threat Hunting* demonstram potencial significativo para elevar a resiliência sistêmica. Contudo, esses instrumentos só produzem efeitos estruturantes quando incorporados a políticas públicas indutoras, com padronização nacional, incentivos regulatórios e integração institucional.

Por fim, a análise crítica da literatura sociológica alerta para os efeitos colaterais das políticas de segurança excessivamente militarizadas. A instrumentalização das ICs como mecanismos de controle territorial interno e a intensificação da violência estatal podem, paradoxalmente, fortalecer a governança criminal e ampliar a assimetria entre Estado e atores ilegais. Assim, uma implicação central é que políticas públicas orientadas exclusivamente por uma lógica coercitiva tendem a ser insuficientes e potencialmente contraproducentes, exigindo abordagens que articulem segurança, inteligência, regulação e legitimidade social.

Em síntese, a proteção das ICs no Brasil demanda políticas públicas integradas, permanentes e estrategicamente orientadas, capazes de articular centralização institucional, cooperação público-privada, regulação econômica soberana, coordenação internacional, modernização tecnológica e responsabilidade sociopolítica. Sem essa abordagem sistêmica, o país permanecerá respondendo a crises pontuais, enquanto vulnerabilidades estruturais continuam a comprometer a segurança e a continuidade dos serviços essenciais.

REFERÊNCIAS

ANNIBAL, Mariana Parmezan. O reconhecimento das organizações criminosas como estrutura complexa e única da sociedade – comparativo à legislação italiana que tipifica nominalmente o pertencimento a uma associação criminosa (ART. 416-BIS). **ReJuB - Rev. Jud. Bras.**, Brasília, Ano 2, n. 1, p. 411-440, jan./jul. 2022. Disponível em: https://revistadaenfam.emnuvens.com.br/renfam/article/view/189. Acesso em 22 de fevereiro de 2026.

LOZANO, Mario Aragonés; LLOPIS, Israel Pérez; DOMINGO, Manuel Esteve. Threat Hunting Architecture Using a Machine Learning Approach for Critical Infrastructures

Protection. **Big Data Cogn. Comput.** 2023, 7, 65. Disponível em: https://doi.org/10.3390/bdcc7020065. Acesso em 20 de janeiro de 2026.

BADIN, Michelle Ratton Sanchez; KROETZ, Maria Eugênia do Amaral; MORAIS, Ana Maria; MISRA, Manu. Infraestrutura crítica e o controle de investimento externo : a regulação do Brasil em contraste. **Boletim de Economia e Política Internacional**, Brasília, DF: Ipea, n. 36, p. 27-58, maio/ago. 2023. Disponível em: http://dx.doi.org/10.38116/bepi36art2. Acesso em 18 de janeiro de 2026.

BRASIL. **Decreto nº 10.569, de 9 de dezembro de 2020**. Aprova a Estratégia Nacional de Segurança de Infraestruturas Críticas. Presidência da República, 2020a. Disponível em: https://www.planalto.gov.br/cCivil_03/_Ato2019-2022/2020/Decreto/D10569.htm. Acesso em: 27 de setembro de 2025.

BRASIL. **Estratégia Nacional de Defesa**. Governo Federal, 2020b. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/pnd_end_congresso_1.pdf. Acesso em 27 de fevereiro de 2026.

BRASIL. **Decreto nº 11.200, de 15 de setembro de 2022**. Aprova o Plano Nacional de Segurança de Infraestruturas Críticas. Brasília, DF: Presidência da República, 2022a. Disponível em: http://www.planalto.gov.br. Acesso em 26 de fevereiro de 2026).

BRASIL. **Ministério da Justiça e Segurança Pública**. Relatório Nacional sobre Crime Organizado. Brasília, DF: Ministério da Justiça e Segurança Pública, 2022b. Disponível em: https://www.gov.br/mj. Acesso em: 27 de fevereiro de 2026.

BRASIL. **Decreto nº 11.856, de 26 de dezembro de 2023**. Institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança. Presidência da República, 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11856.htm. Acesso em 27 de fevereiro de 2026.

BRASIL. **Decreto nº 9.573, de 22 de novembro de 2018**. Aprova a Política Nacional de Segurança de Infraestruturas Críticas. Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Decreto/D9573.htm. Acesso em 27 de fevereiro de 2026.

BRASIL. **Decreto-Lei nº 2848 de 7 de dezembro de 1940**. Código Penal. Presidência da República, 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em 1 de outubro de 2025.

BRASIL. **Lei nº 12.850, de 2 de agosto de 2013**. Define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal. Presidência da República, 2013. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm. Acesso em 1 de outubro de 2025.

BRASIL. **Lei nº 13.260, de 16 de março de 2016**. Regulamenta o disposto no inciso XLIII do art. 5º da Constituição Federal, disciplinando o terrorismo, tratando de disposições investigatórias e processuais e reformulando o conceito de organização terrorista. Presidência da República, 2016. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/lei/l13260.htm. Acesso em 1 de outubro de 2025.

BRASIL. **Portaria Interministerial GSI-PR/MAPA/MCID/MCTI/MD/MF/MGI/MIDR/MJSP/MS nº 4, de 21.11.2024**. Institui o Comitê Nacional de Segurança de Infraestruturas Críticas no âmbito da Câmara de Relações Exteriores e Defesa Nacional do Conselho de Governo. Disponível em: https://antigo.mctic.gov.br/mctic/opencms/legislacao/portarias_interministeriais/Portaria_Interministerial_GSIPR_MAPA_MCID_MCTI_MD_MF_MGI_MIDR_MJSP_MS_n_4_de_21112024.html. Acesso em: 1 de outubro de 2025.

BMI (Bundesministerium des Innern und Für Heimat). **Cyber Security Strategy for Germany. Berlin**, 2021. Disponível em: https://www.bmi.bund.de/SharedDocs/downloads/EN/themen/it-digital-policy/cyber-security-strategy-for-germany2021.pdf. Acesso em: 27 de fevereiro 2026

CAMARGO, Beatriz Corrêa; SILVEIRA, Renato de Mello Jorge. Organização criminosa sem crime? Observações críticas sobre a proposta de reforma pelo Projeto de Lei Anticrime. **Instituto Brasileiro de Ciências Criminais**. Boletim - 317 - Esp. Pac. Anticrime, 2020. Disponível em: https://arquivo.ibccrim.org.br/boletim_artigo/6315-Organizacao-criminosa-sem-crime-Observacoes-criticas-sobre-a-proposta-de-reforma-pelo-Projeto-de-Lei-Anticrime. Acesso em 22 de fevereiro de 2026.

DAOUSIS, S.; PELADARINOS, N.; CHEIMARAS, V.; PAPAGEORGAS, P.; PIROMALIS, D.D.; MUNTEANU, R.A. Overview of Protocols and Standards for Wireless Sensor Networks in Critical Infrastructures. **Future Internet 2024**, 16, 33. Disponível em: https://doi.org/10.3390/fi16010033. Acesso em 06 de janeiro de 2026.

EUROPEAN COMMISSION. Critical Infrastructure: Staff Working Document accompanying the Communication on enhancing critical infrastructure resilience, including protection of network and information systems. EUR-Lex, **Doc. COM(2020) 829 final**, 18 dez. 2020. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020SC0358. Acesso em: 27 de fevereiro de 2026.

EU (European Union). Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. **Official Journal of the European Union**, L 194, p. 1–30, 19 jul. 2016. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L1148. Acesso em: 27 de fevereiro de 2026.

EU (European Union). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across

the Union (NIS2 Directive), repealing Directive (EU) 2016/1148. **Official Journal of the European Union**, L 333, p. 80–152, 27 dez. 2022. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555. Acesso em: 27 de fevereiro de 2026.

EUROPOL. European Union Serious and Organised Crime Threat Assessment (SOCTA) 2021. **Luxembourg: Publications Office of the European Union**, 2021. Disponível em: https://www.europol.europa.eu. Acesso em: 27 de fevereiro de 2026.

EUROPOL. European Union Terrorism Situation and Trend Report (TE-SAT) 2022. **Luxembourg: Publications Office of the European Union**, 2022. Disponível em: https://www.europol.europa.eu. Acesso em: 27 de fevereiro de 2026.

FBSP (Fórum Brasileiro de Segurança Pública). **17º Anuário Brasileiro de Segurança Pública**. São Paulo: Fórum Brasileiro de Segurança Pública, 2023. Disponível em: https://forumseguranca.org.br/wp-content/uploads/2023/07/anuario-2023.pdf. Acesso em: 27 de fevereiro de 2026.

SIQUEIRA, Ítalo Barbosa Lima; NASCIMENTO; Francisco Elionardo de Melo; MORAES, Suiany Silva. Inter-Regional Dynamics of Markets and Criminal Governance in Fortaleza and Manaus in Comparative Perspective. **Dilemas. Revista de Estudos de Conflito e Controle Social**. Edição Especial 4 - 'Governança Criminal na América Latina em Perspectiva Comparada', 2022. Disponível em https://revistas.ufrj.br/index.php/dilemas/article/view/52526. Acesso em 28 de dezembro de 2025.

FERREIRA, Hugo José Duarte. Identificação e caracterização de infraestruturas críticas: Uma metodologia. **Cadernos do IUM**, N.º 14, Maio 2017. Disponível em: https://www.ium.pt/files/publicacoes/Cadernos/14/Cadernos_IUM_14_Infraestruturas_Criticas.pdf. Acesso em 05 de janeiro de 2026.

GOVEA, J.; GAIBOR-NARANJO, W.; VILLEGAS-CH, W. Securing Critical Infrastructure with Blockchain Technology: An Approach to Cyber-Resilience. **Computers**, v. 13, n. 5, 122, 2024. Disponível em: https://doi.org/10.3390/computers13050122. Acesso em 06 de janeiro de 2026.

GÜLCAN, T. A.; ERGINER, K. E.. National and international maritime situational awareness model examples and the effects of North Stream Pipelines sabotage. **International Journal of Critical Infrastructure Protection**, 2023. Disponível em: https://ideas.repec.org/a/eee/ijocip/v42y2023ics1874548223000379.html. Acesso em 05 de janeiro de 2026.

GUTERRES, E. C. Regulação de Riscos e Proteção de Infraestruturas Críticas: os novos ventos do fenômeno regulatório. **Revista de Direito Setorial e Regulatório**, v. 2, n. 1, 107-160, 2016. Disponível em: https://periodicos.unb.br/index.php/rdsr/article/view/19254. Acesso em 15 de janeiro de 2026.

INÁCIO, Tiago Viesba Pini; SILVA, Márcia da. Geopolítica Militar Brasileira e a Segurança das Infraestruturas Críticas: a estratégia de gestão de um novo sistema territorial. In: **XV**

Encontro Nacional de Pós-Graduação e Pesquisa em Geografia, 2023. Disponível em: https://ojs.ufgd.edu.br/anpege/article/view/18921. Acesso em 15 de janeiro de 2026.

ISO 22316:2017. **Security and resilience — Organizational resilience — Principles and attributes**, 2017. Disponível em: https://www.iso.org/standard/50053.html. Acesso em 27 de fevereiro de 2026.

JUNGWIRTH, R., Smith, H., Willkomm, E., Savolainen, J., Alonso Villota, M. et al., Hybrid Threats: A Comprehensive Resilience Ecosystem, **Publications Office of the European Union**, Luxembourg, 2023. Disponível em: https://data.europa.eu/doi/10.2760/37899. Acesso em 28 de fevereiro de 2026.

LOZANO, Mario Aragonés; LLOPIS, Israel Pérez; DOMINGO, Manuel Esteve. Threat Hunting Architecture Using a Machine Learning Approach for Critical Infrastructures Protection. **Big Data Cogn. Comput**. 2023, 7, 65. Disponível em: https://doi.org/10.3390/bdcc7020065. Acesso em 12 de janeiro de 2026.

MIOVSKA, Leta Bardžieva. Hybrid Threats and a Comprehensive Approach to Addressing Them. **Security Challenges, Risks And Threats of the 21st Century - A Multidisciplinary Approach**. Faculty of Business Studies and Law Union-Nikola Tesla" University, Belgrade, Republic of Serbia. 2022. Disponível em: https://www.caruk.rs/wp-content/uploads/Studentski-tematski-Zbornik-radova.pdf#page=143. Acesso em 27 de fevereiro de 2026.

MIRANDA FILHO, F. N. O Papel do Serviço de Inteligência na Segurança das Infraestruturas Críticas. **Revista Brasileira de Inteligência**, v. 7, 79-92, 2012. Disponível em: https://rbi.abin.gov.br/RBI/article/view/97. Acesso em 22 de fevereiro de 2026.

NEVES, Tiago Duarte. Infraestruturas críticas e ameaças cibernéticas: uma análise da cibersegurança dos cabos submarinos brasileiros. **Escola Superior de Guerra**, 2024. Disponível em: https://repositorio.esg.br/handle/123456789/1979. Acesso em 23 de janeiro de 2026.

NONATO, Marcos Paulo Cardoso; PINHO, Harley de. A integração do Sistema Militar de Defesa Cibernética (SMDC) com a proteção cibernética das infraestruturas críticas de interesse para Defesa Nacional. **Escola Superior de Defesa**, Brasília, 2021. Disponível em: https://repositorio.esg.br/handle/123456789/1426. Acesso em 10 de fevereiro de 2026.

OECD – Organisation for Economic Co-operation and Development. Good Governance for Critical Infrastructure Resilience. **OECD Reviews of Risk Management Policies**, Paris: OECD Publishing, 2019. Disponível em: https://doi.org/10.1787/02f0e5a0-en. Acesso em: 27 de fevereiro 2026.

OKABAYASHI, Victor Hugo. **Defesa Cibernética em infraestruturas críticas: estratégias avançadas para mitigação de ameaças**. Rio de Janeiro: ESG, 2024. Disponível em: https://repositorio.esg.br/bitstream/123456789/2081/1/CAEPE.82%202024%20TCC%20VF%20assinado.pdf. Acesso em 22 de fevereiro de 2026.

OLIVEIRA, David Medeiros; ANDRADE, Donizeti de; MONTEIRO, Arthur Maximus. Intelligence and Airport Security: A SWOT Analysis of the Brazilian Scenario. Thematic Section Aviation Safety and Continued Airworthiness. **J. Aerosp. Technol. Manag**. 14, 2022. Disponível em: https://doi.org/10.1590/jatm.v14.1275. Acesso em 22 de fevereiro de 2026.

PESTANA, G.; SOFOU, S. Data Governance to Counter Hybrid Threats against Critical Infrastructures. **Smart Cities**, 7, 1857–1877, 2024. Disponível em: https://www.mdpi.com/2624-6511/7/4/72. Acesso em 28 de fevereiro de 2026.

RAMOS JUNIOR, Humberto Ferreira. A inteligência cibernética e a proteção das infraestruturas críticas de interesse do país. **Escola Superior de Guerra**, 2024. Disponível em: https://repositorio.esg.br/handle/123456789/2042. Acesso em 10 de fevereiro de 2026.

RAMOS, Leonardo; ROCHA, Pedro D.; ZAHREDDINE, Danny. A Agenda de Segurança Internacional no BRICS (2009-2019). **Dados**, Rio de Janeiro, v. 64, n. 3, e20190244, 2021. Disponível em: https://www.scielo.br/j/dados/a/hwsnG9nrPWfYRVQghVWGd8h/?format=pdf&lang=pt. Acesso em 22 de fevereiro de 2026.

SÁ, Odair Oliveira de. **A segurança das infraestruturas críticas de energia no Brasil**. Programa de Pós-Graduação em Energia, Universidade de São Paulo, São Paulo, 2017. Disponível em: https://teses.usp.br/teses/disponiveis/106/106131/tde-04122017-150226/pt-br.php. Acesso em 22 de fevereiro de 2026.

SALLA, Fernando; TEIXEIRA, Alessandra. O crime organizado entre a criminologia e a sociologia: Limites interpretativos, possibilidades heurísticas. **Dossiê - Sociologia e Criminologia: Sobreposições, Tensões e Conflitos • Tempo social**. v. 32, n. 3, 2020. Disponível em: https://www.scielo.br/j/ts/a/K7HHBqvBchTkKdwLVjybDwb/?format=html&lang=pt. Acesso em 22 de fevereiro de 2026.

SILVA, Eduardo Luís Gonçalves Pequeno de Oliveira e. Cibersegurança das Infraestruturas Críticas Nacionais. Academia da Força Aérea, **Sintra**, 2015. Disponível em: https://comum.rcaap.pt/entities/publication/2f1be4ab-33c2-49e0-b8f0-611d32005a09. Acesso em 18 de fevereiro de 2026.

UDEANU, Gheorghe. Opinions Regarding The New Challenges To The Critical Infrastructures. In: **International Conference Knowledge-Based Organization**. v. XXI, n. 1, 2015. Disponível em: https://reference-global.com/download/article/10.1515/kbo-2015-0021.pdf. Acesso em 22 de fevereiro de 2026.

UNODC (United Nations Office on Drugs and Crime). **The Crime–Terror Nexus: Challenges and Responses**. Vienna: United Nations, 2019. Disponível em: https://www.unodc.org. Acesso em: 27 de fevereiro de 2026.

UNODC (United Nations Office on Drugs and Crime). **Global Report on Organized Crime 2023**. Vienna: United Nations, 2023. Disponível em: https://www.unodc.org. Acesso em: 27 de fevereiro de 2026.

UNITED STATES. Critical Infrastructure Security and Resilience Month, 2023. **Proclamation 10660 of October 31, 2023**. Federal Register, Washington, DC, 3 nov. 2023. Disponível em: https://www.federalregister.gov/documents/2023/11/03/2023-24482/critical-infrastructure-security-and-resilience-month-2023. Acesso em: 27 de fevereiro de 2026.

UNITED STATES. Cybersecurity and Infrastructure Security Agency Act of 2018. **Public Law 115-278, 16 nov. 2018.** Disponível em: https://www.govinfo.gov/content/pkg/COMPS-15296/pdf/COMPS-15296.pdf. Acesso em: 27 de fevereiro de 2026.

UNITED STATES. Government at a Glance 2023 Country Notes. **Organisation for Economic Co-operation and Development (OECD)**, 2023. Disponível em: https://www.oecd.org/en/publications/government-at-a-glance-2023_c4200b14-en/united-states_015a6beb-en.html. Acesso em 27 de fevereiro de 2026.

VIEIRA, Henrique Primo. A Defesa das Infraestruturas Críticas Brasileiras à Luz Dos Normativos e dos Objetivos do Exercício Guardião Cibernético: Uma Análise Construtiva. **Escola Superior de Defesa (ESD),** 2023. Disponível em: https://repositorio.esg.br/handle/123456789/1781. Acesso em 28 de fevereiro de 2026.

WANG, Shuliang; GU, Xifeng; LUAN, Shengyang; ZHAO, Mingwei. Resilience analysis of interdependent critical infrastructure systems considering deep learning and network theory. **International Journal of Critical Infrastructure Protection**. v. 35, 2021. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S1874548221000500?via%3Dihub. Acesso em 2 de março de 2026.

WENDT, Emerson. Ciberguerra, Inteligência Cibernética e Segurança Virtual: alguns aspectos. **Revista Brasileira de Inteligência**, n. 6, abr. 2011, pp. 15-26. Disponível em: https://rbi.abin.gov.br/RBI/article/view/80. Acesso em 20 de fevereiro de 2026.

ZILIO, Jacson. O Conceito de Organização Criminosa: Entre Fantasia e Expansão do Poder Punitivo. **Revista do Sistema Único de Segurança Pública**, Brasília, Brasil, v. 4, n. 2, p. 159–182, 2025. DOI: 10.56081/revsusp.v4i2.657. Disponível em: https://revistasusp.mj.gov.br/susp/index.php/revistasusp/article/view/657. Acesso em: 22 de fevereiro de 2026.

APÊNDICE A

Quadro 3: Matriz de síntese resultante da revisão integrativa

Artigo (Referência)	**Tipo**	**a) Tipo de Estudo e Metodologia Principal**	**b) Foco Geopolítico e Nível de Análise**	**c) Atores Criminosos e Estrutura Analisada**	**d) Modus Operandi e Alvos de Infraestrutura Crítica**	**e) Principais Achados e Impacto Medido**	**f) Conclusões e Implicações para Políticas Públicas**
Sá (2017)	Dissertação	Dissertação (revisão bibliográfica e análise documental) focada em fontes secundárias sobre segurança energética e gestão de riscos.	Foco nacional (Brasil), analisando a segurança energética do país e propondo parâmetros de criticidade para infraestruturas de energia.	Discute ameaças genéricas como terrorismo, crime organizado, falhas humanas e desastres naturais, mas não detalha a estrutura de grupos criminosos específicos.	Descreve modus operandi de ataques globais (ex: FARC na Colômbia, Stuxnet no Irã) e desastres naturais, focando em oleodutos, subestações e sistemas SCADA de energia.	O principal achado é a proposição de parâmetros para classificação de ICs de energia no Brasil (elétrico e petróleo) e a sugestão de monitoramento orbital.	Conclui sobre a necessidade de modernizar a legislação, fortalecer a cultura de prevenção e propõe políticas públicas para gestão integrada de riscos.
Silva (2015)	Dissertação	Dissertação (qualitativa) que utiliza análise documental (leis, diretivas UE/NATO) e entrevistas semiestruturadas com especialistas militares e civis portugueses.	Foco nacional (Portugal), analisando a estrutura de cibersegurança e o potencial papel das Forças Armadas (FFAA) na proteção das Infraestruturas Críticas Nacionais (ICN).	Discute ameaças genéricas (terroristas, crime organizado, Estados, indivíduos) e foca na estrutura estatal de resposta (FFAA, CNCS, ANPC).	Define ameaças cibernéticas (ativas e passivas) e classifica os domínios de atuação (proteção, prossecução criminal, defesa do Estado), sem detalhar ataques específicos a ICs.	O principal achado é que as metodologias de gestão de risco (ISO 31000, RAMCAP) devem ser aplicadas pelas entidades responsáveis (ANPC, CNCS) na definição dos requisitos de segurança.	Conclui que as FFAA têm um papel na cibersegurança das ICNs (além da ciberdefesa) e recomenda que apoiem o CNCS e a ANPC na definição de requisitos de segurança.

Oliveira (2022)	Tese	Tese (qualitativa) que realiza uma análise comparativa da governança cibernética, focada em documentos estratégicos e legislação.	Foco transnacional (Brasil e Reino Unido), comparando as governanças cibernéticas de ambos, com ênfase específica nas infraestruturas críticas marítimas (ICM).	Aborda ameaças de forma ampla (hackers, ciberterroristas) e cita o ataque de ransomware à A.P. Moller-Maersk como exemplo de ator criminoso.	Descreve o ataque de ransomware NotPetya contra a A.P. Moller-Maersk em 2017, que interrompeu operações em 76 terminais portuários globalmente.	O estudo comparativo conclui que o Reino Unido possui uma governança mais madura, com estratégias, normas (Regulamentos NIS, CAF) e órgãos (NCSC) específicos para ICs marítimas.	Conclui que o Brasil carece de uma governança cibernética específica para ICMs e recomenda a elaboração de uma Estratégia de Segurança Marítima.
Nonato e Pinho (2021)	Artigo	Artigo (qualitativo) baseado em pesquisa bibliográfica e análise documental da legislação brasileira de defesa e segurança cibernética.	Foco nacional (Brasil), analisando a integração do Sistema Militar de Defesa Cibernética (SMDC) com a proteção cibernética das infraestruturas críticas (ICs).	Discute ameaças de forma genérica (ataques a estruturas estratégicas) e foca na estrutura estatal (SMDC, GSI/PR).	Cita ataques históricos (Estônia 2007, Stuxnet 2009, Ucrânia 2015, Colonial Pipeline 2021) contra ICs (bancos, nuclear, energia, oleodutos) para contextualizar a ameaça.	Constata que as iniciativas de integração no Brasil (ex: Exercício Guardião Cibernético) são incipientes e carecem de uma estrutura nacional que normatize e integre as capacidades do SMDC e das ICs.	Propõe a criação de um Centro Nacional de Segurança Cibernética (CNSC-BRASIL) vinculado ao GSI/PR para coordenar a proteção cibernética nacional e a integração do SMDC.
Inácio e Silva (2023)	Artigo	Artigo de conferência (qualitativo) que utiliza revisão bibliográfica, análise de documentos oficiais (GSI) e dados de militarização para analisar o pensamento	Foco nacional (Brasil), analisando como o pensamento geopolítico militar influenciou as políticas de defesa territorial e de ICs no Governo Jair Bolsonaro.	Não declarado (o foco é na estrutura de gestão estatal, especificamente a militarização do GSI e a "tutela" das FA sobre o território).	Não declarado (o foco é na política de proteção e gestão das ICs, não em ataques específicos contra elas).	Mapeia 644 ICs no Brasil, constatando que o programa de SIC foi centralizado no GSI (militarizado) e focado nas regiões Sudeste, Sul e Nordeste (70% das ICs).	Conclui que as ICs são um objetivo estratégico militar para garantir o controle político do território e da população, refletindo um projeto geopolítico de aplicação interna.

		geopolítico militar.					
Ramos Júnior (2024)	Monografia	Monografia (qualitativa) baseada em análise documental e revisão bibliográfica do arcabouço normativo brasileiro sobre cibersegurança e ICs.	Foco nacional (Brasil), analisando a estrutura de defesa cibernética (SMDC, ABIN) e a proteção das infraestruturas críticas (IC) do país.	Discute ameaças de forma ampla (hackers, criminosos, grupos especializados patrocinados e estados-nação) e foca na estrutura estatal (ABIN, SMDC, futura ANCiber).	Descreve técnicas de ataque (DDoS , ransomware, spear-phishing , APT) e incidentes históricos (Stuxnet, Black Energy 3 , NotPetya, SolarWinds, Ministério da Saúde contra ICs (energia, saúde, nuclear).	O principal achado é a identificação da necessidade de uma Agência Nacional de Cibersegurança (ANCiber) para coordenar o compartilhamento de informações entre setores público e privado.	Conclui que a criação da ANCiber, colaborando com a ABIN e o SMDC, é uma ação estratégica essencial para fortalecer a proteção das ICs nacionais através do compartilhamento de inteligência.
Wendt (2011)	Artigo	Artigo de periódico (conceitual) que explora a ciberguerra e propõe o conceito de "Inteligência Cibernética" com base em análise de cenário.	Foco nacional (Brasil) e internacional, analisando a segurança virtual no cenário brasileiro e global e propondo um método de inteligência.	Analisa atores de forma genérica (indivíduo, grupo, organização, Estado), classificando-os por motivação (cibervandalismo, cibercrime, ciberespionagem, ciberterrorismo, ciberguerra).	Descreve ataques a infraestruturas críticas (energia, água, transporte, bancos, nuclear) e cita o Stuxnet como exemplo de ciber-arma contra sistemas SCADA.	Propõe o conceito de "Inteligência Cibernética" como um processo de produção de conhecimento prospectivo sobre ameaças virtuais para subsidiar decisões de defesa e resposta.	Conclui que o Brasil, carente de regras claras, necessita de um debate sobre Inteligência Cibernética envolvendo todos os setores (público e privado) para prevenir e reagir a ameaças.
Ramos, Rocha e Zahreddine (2021)	Artigo	Artigo de periódico (qualitativo e quantitativo) que utiliza análise de conteúdo das declarações de cúpula do BRICS (2009-2019).	Foco transnacional (BRICS), analisando a evolução da agenda de segurança do grupo em suas cúpulas anuais.	Analisa como o BRICS discute atores criminosos, focando em "terrorismo", "crime organizado transnacional" e "tráfico de drogas" como categorias temáticas.	Discute o "terrorismo" e o "crime cibernético" como ameaças, mencionando o uso de Tecnologias de Informação e Comunicação (ICTs) por terroristas e a	Constata que a segurança internacional tornou-se central na agenda do BRICS, com "Paz e Resolução de Conflitos" e "Terrorismo" sendo os temas mais	Conclui que a cooperação em segurança no BRICS é impulsionada tanto pelo nexo desenvolvimento-segurança quanto por interesses particulares dos membros (ex:

					necessidade de proteger infraestruturas críticas.	frequentes.	Rússia sobre Ucrânia).
Ferreira (2017)	Artigo	Artigo de periódico (qualitativo-comparativo) que analisa documentos legais e metodologias de proteção de IC.	Foco transnacional, comparando a metodologia de identificação de IC de Portugal com a da UE, Espanha, Reino Unido, EUA e Canadá.	Analisa ameaças de forma ampla (terrorismo transnacional, ciberterrorismo, cibercriminalidade, riscos naturais) como justificativa para a proteção de IC.	Não declarado (o foco é na metodologia de identificação e proteção, não em ataques específicos).	O principal achado é uma proposta de metodologia aprimorada para Portugal, sugerindo novos setores (Governação, Monumentos) e critérios (Redundância, Impacto Geográfico).	Conclui que Portugal deve aplicar uma metodologia de identificação e caracterização de IC mais abrangente na primeira fase de elaboração do seu Programa Nacional de Proteção.
Badin, Kroetz, Morais, Misra (2023)	Artigo	Artigo de periódico (qualitativo) que realiza análise bibliográfica e documental da legislação brasileira e do direito comparado (EUA, Alemanha, China) sobre investimento externo.	Foco nacional (Brasil) e internacional, analisando a ausência de controle de investimentos externos em infraestruturas críticas no Brasil.	Não declarado (o foco é no investidor externo como um risco potencial, não em grupos criminosos).	Não declarado (discute o risco de controle/propriedade de ICs por entidades estrangeiras, não ataques físicos ou cibernéticos).	Constata que o Brasil, diferentemente de outras potências, não possui um mecanismo de triagem (screening) para investimentos externos em ICs, gerando vulnerabilidade estratégica.	Conclui pela necessidade de o Brasil implementar um mecanismo de controle de investimento estrangeiro em suas ICs, alinhado à segurança nacional, sem adotar o protecionismo.
Oliveira, Andrade e Monteiro (2022)	Artigo	Estudo qualitativo utilizando a Matriz SWOT para analisar o cenário da segurança aeroportuária brasileira,	Foco geopolítico nacional no Brasil, analisando o impacto da concessão de aeroportos à iniciativa privada na	O artigo caracteriza os atores como crime organizado transnacional e grupos capazes de ciberataques, mencionando facções	Descreve o modus operandi envolvendo roubos de carga de alto valor com armamento pesado e veículos falsificados em terminais, além de	Identifica um vácuo legal no compartilhamento de inteligência com aeroportos privados, citando impactos financeiros de	Conclui pela necessidade urgente de protocolos de compartilhamento de dados sigilosos com entes privados e treinamento

		baseando-se em documentos governamentais (PNI, PNAVSEC), legislação e relatórios de riscos globais (WEF).	infraestrutura crítica e a relação com o Sistema Brasileiro de Inteligência (SISBIN).	criminosas que controlam fluxos ilícitos e influenciam infraestruturas críticas a partir de presídios	ciberataques visando interromper redes de infraestrutura crítica.	grandes roubos (720 kg de ouro) e a alta severidade potencial de ciberataques na matriz de riscos.	especializado em inteligência para mitigar vulnerabilidades decorrentes das concessões.
Siqueira, Nascimento, Moraes (2022)	Artigo	Artigo de periódico (qualitativo/etnográfico) que analisa mercados de drogas e governança criminal por meio de entrevistas, observação e análise de dados secundários.	Foco local (Brasil), comparando as dinâmicas criminais e mercados em Fortaleza (CE) e Manaus (AM) em perspectiva inter-regional.	Detalha a estrutura de grupos criminosos (PCC, CV, FDN), analisando suas hierarquias, regras (estatutos), financiamento (tráfico) e governança normativa nos territórios.	Não declarado (o foco é na governança criminal e mercados de drogas, não em ataques a infraestruturas críticas).	Constata que as facções regulam mercados ilícitos (drogas, armas) e lícitos (gás, transporte), exercendo governança sobre a vida urbana e conflitos.	Conclui que a violência estatal é um fator central na regulação desses mercados e que as facções criaram uma ordem social normativa própria, paralela ao Estado.
Gülcan, Erginer (2023).	Artigo	Artigo de periódico (análise qualitativa) que examina a evolução da consciência situacional marítima (MSA) na UE, usando análise documental de políticas e projetos.	Foco regional (União Europeia) e internacional, analisando os desafios técnicos e políticos para criar um sistema integrado de vigilância marítima (CISE).	Não declarado (o foco é na vigilância marítima para combater pirataria e crime, mas não analisa a estrutura desses atores).	Discute a necessidade de vigilância contra o terrorismo, pirataria, tráfico de drogas e armas, e despejo ilegal de resíduos no mar, mas não detalha modus operandi de ataques.	Constata que, apesar dos avanços tecnológicos, a UE enfrenta fragmentação política e barreiras legais (soberania) para implementar um sistema de vigilância marítima comum (CISE).	Conclui que a UE deve superar a fragmentação setorial e as barreiras de soberania para alcançar uma consciência situacional marítima eficaz e compartilhada.
Miranda Filho (2012)	Artigo	Artigo de periódico (ensaio/análise qualitativa) que discute o papel da Inteligência na	Foco nacional (Brasil), analisando a importância da atividade de Inteligência para a	Discute ameaças de forma ampla (terrorismo, crime organizado, espionagem,	Não declarado (discute ameaças de forma teórica, sem detalhar modus operandi ou ataques	O principal achado é que a Inteligência é crucial para a SIC, fornecendo conhecimento	Conclui que a atividade de Inteligência é a ferramenta mais eficaz para a SIC,

		proteção de ICs, baseado em análise conceitual e doutrinária.	Segurança das Infraestruturas Críticas (SIC) no país.	sabotagem) e atores estatais e não estatais como riscos às ICs.	específicos).	antecipado sobre ameaças e vulnerabilidades para subsidiar a tomada de decisão.	defendendo a integração do SISBIN e a cooperação público-privada.
Udeanu (2015)	Artigo	Artigo de periódico (análise qualitativa) que examina as novas ameaças (híbridas, cibernéticas, pandêmicas) às ICs, com base em revisão bibliográfica e análise de cenário.	Foco internacional (perspectiva global/OTAN/UE), analisando os desafios emergentes para a resiliência das infraestruturas críticas.	Discute atores estatais (Rússia, China) e não estatais (terroristas) que utilizam táticas híbridas e cibernéticas para atacar ICs.	Descreve o modus operandi de ataques híbridos, combinando guerra cibernética, desinformação e ataques físicos (ex: drones) contra ICs (energia, transporte, saúde, espaço).	O principal achado é que as ICs estão vulneráveis a ameaças híbridas complexas (ex: COVID-19, ataques cibernéticos coordenados) que exploram a interdependência sistêmica.	Conclui que a proteção de ICs exige uma abordagem de "resiliência por design", cooperação público-privada e maior coordenação entre UE e OTAN.
Daousis, Peladarinos, Cheimaras, Papageorgas, Piromalis, Munteanu (2024)		Artigo de revisão (qualitativo) que analisa e compara protocolos e padrões de redes de sensores sem fio (WSN) para ICs.	Foco técnico/global, analisando padrões (ex: ZigBee, WirelessHART, ISA100.11a) aplicáveis a Redes de Sensores Sem Fio em infraestruturas críticas.	Não declarado (foco estritamente técnico nos protocolos).	Discute a vulnerabilidade de WSNs a ataques como jamming, spoofing e ataques de negação de serviço (DoS) que visam a infraestrutura de monitoramento.	O principal achado é uma comparação detalhada das características, vantagens e limitações dos principais padrões WSN para aplicações industriais e de IC.	Conclui que padrões como ISA100.11a e WirelessHART oferecem maior segurança e interoperabilidade para o monitoramento de ICs, mas a escolha depende da aplicação específica.
Guterres (2016)	Artigo	Artigo de periódico (ensaio/análise qualitativa) que analisa a evolução da regulação de riscos e proteção de ICs no Brasil, usando	Foco nacional (Brasil), analisando o desenvolvimento do arcabouço regulatório de proteção de ICs (CIP), impulsionado	Não declarado (foco na regulação estatal, não em atores criminosos).	Não declarado (discute o risco de forma regulatória, não modus operandi de ataques).	Constata que o programa de CIP no Brasil "nasceu crescido", adotando a abordagem "all-hazards" (contra todos os riscos) e foi	Conclui que a regulação de riscos para ICs no Brasil, embora recente, avançou rapidamente devido aos grandes eventos, integrando-se

		análise documental e direito comparado.	por grandes eventos (Copa, Olimpíadas).			impulsionado por eventos (Pan 2007, Copa 2014).	à lógica da defesa civil.
Govea, Gaibor-Naranjo, Villegas-Ch (2024)	Artigo	Artigo de revisão (qualitativo) que explora a aplicação da tecnologia blockchain para a segurança de ICs, analisando literatura existente.	Foco técnico/global, analisando como o blockchain pode proteger diversos setores de infraestrutura crítica (energia, saúde, transporte).	Não declarado (foco na tecnologia de defesa).	Descreve ameaças cibernéticas (ex: ataques Man-in-the-Middle, DoS, falsificação de dados) que podem comprometer sistemas de controle industrial (ICS) e redes elétricas inteligentes (Smart Grids).	O principal achado é que o blockchain pode aumentar a segurança das ICs ao prover descentralização, imutabilidade e transparência, dificultando ataques cibernéticos.	Conclui que o blockchain é uma solução promissora para os desafios de segurança das ICs, embora enfrente desafios de escalabilidade e complexidade de implementação.
Lozano, Llopis, Domingo (2023)	Artigo	Artigo de conferência (quantitativo/técnico) que propõe uma arquitetura de Threat Hunting usando Machine Learning (LSTM-AE) e dados de sistemas SCADA.	Foco técnico/global, desenvolvendo uma arquitetura de detecção de anomalias para sistemas de controle industrial (ICS) em infraestruturas críticas.	Não declarado (foco na detecção da ameaça, não no ator).	Modela ameaças como anomalias e ataques cibernéticos (ex: injeção de dados falsos) contra sistemas SCADA, visando a infraestrutura de controle.	O principal achado é uma arquitetura que melhora a detecção de ataques em dados de série temporal de ICs, superando métodos tradicionais em precisão.	Conclui que a arquitetura proposta é eficaz para a detecção proativa de ameaças (threat hunting) em infraestruturas críticas, melhorando a resiliência cibernética.

Fonte: elaborado pelos autores